EKI-7758F

8G ports Industrial Managed Redundant Gigabit Ethernet Switch, 4 Gigabit Copper and 4 Gigabit SFP

User Manual

Copyright

Acknowledgements

Intel and Pentium are trademarks of Intel Corporation.
Microsoft Windows and MS-DOS are registered trademarks of Microsoft Corp.
All other product names or trademarks are properties of their respective owners.

Part No.
Printed in China

2nd Edition
August 2007

Product Warranty (2 years)

Advantech warrants to you, the original purchaser, that each of its products will be free from defects in materials and workmanship for two years from the date of purchase.

This warranty does not apply to any products which have been repaired or altered by persons other than repair personnel authorized by Advantech, or which have been subject to misuse, abuse, accident or improper installation. Advantech assumes no liability under the terms of this warranty as a consequence of such events.

Because of Advantech′s high quality-control standards and rigorous testing, most of our customers never need to use our repair service. If an Advantech product is defective, it will be repaired or replaced at no charge during the warranty period. For out-of-warranty repairs, you will be billed according to the cost of replacement materials, service time and freight. Please consult your dealer for more details.

If you think you have a defective product, follow these steps:

1. Collect all the information about the problem encountered. (For example, CPU speed, Advantech products used, other hardware and software used, etc.) Note anything abnormal and list any onscreen messages you get when the problem occurs.
2. Call your dealer and describe the problem. Please have your manual, product, and any helpful information readily available.
3. If your product is diagnosed as defective, obtain an RMA (return merchandize authorization) number from your dealer. This allows us to process your return more quickly.
4. Carefully pack the defective product, a fully-completed Repair and Replacement Order Card and a photocopy proof of purchase date (such as your sales receipt) in a shippable container. A product returned without proof of the purchase date is not eligible for warranty service.
5. Write the RMA number visibly on the outside of the package and ship it prepaid to your dealer.

Declaration of Conformity

CE

This product has passed the CE test for environmental specifications. Test conditions for passing included the equipment being operated within an industrial enclosure. In order to protect the product from being damaged by ESD (Electrostatic Discharge) and EMI leakage, we strongly recommend the use of CE-compliant industrial enclosure products.

FCC Class A

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Technical Support and Assistance

Step 1. Visit the Advantech web site at **www.advantech.com/support** where you can find the latest information about the product.

Step 2. Contact your distributor, sales representative, or Advantech's customer service center for technical support if you need additional assistance. Please have the following information ready before you call:

- Product name and serial number
- Description of your peripheral attachments
- Description of your software (operating system, version, application software, etc.)
- A complete description of the problem
- The exact wording of any error messages

Safety Instructions

1. Read these safety instructions carefully.
2. Keep this User's Manual for later reference.
3. Disconnect this equipment from any AC outlet before cleaning. Use a damp cloth. Do not use liquid or spray detergents for cleaning.
4. For plug-in equipment, the power outlet socket must be located near the equipment and must be easily accessible.
5. Keep this equipment away from humidity.
6. Put this equipment on a reliable surface during installation. Dropping it or letting it fall may cause damage.
7. The openings on the enclosure are for air convection. Protect the equipment from overheating. DO NOT COVER THE OPENINGS.
8. Make sure the voltage of the power source is correct before connecting the equipment to the power outlet.
9. Position the power cord so that people cannot step on it. Do not place anything over the power cord.
10. All cautions and warnings on the equipment should be noted.
11. If the equipment is not used for a long time, disconnect it from the power source to avoid damage by transient over voltage.
12. Never pour any liquid into an opening. This may cause fire or electrical shock.
13. Never open the equipment. For safety reasons, the equipment should be opened only by qualified service personnel.
14. If one of the following situations arises, get the equipment checked by service personnel:
    a. The power cord or plug is damaged.
    b. Liquid has penetrated into the equipment.
    c. The equipment has been exposed to moisture.
    d. The equipment does not work well, or you cannot get it to work according to the user's manual.
    e. The equipment has been dropped and damaged.
    f. The equipment has obvious signs of breakage.

15. DO NOT LEAVE THIS EQUIPMENT IN AN ENVIRONMENT WHERE THE STORAGE TEMPERATURE MAY GO BELOW -40℃ (-40℉) OR ABOVE 85℃ (185℉). THIS COULD DAMAGE THE EQUIPMENT. THE EQUIPMENT SHOULD BE IN A CONTROLLED ENVIRONMENT.

Safety Precaution - Static Electricity

Follow these simple precautions to protect yourself from harm and the products from damage.

1. To avoid electrical shock, always disconnect the power from your PC chassis before you work on it. Don't touch any components on the CPU card or other cards while the PC is on.
2. Disconnect power before making any configuration changes. The sudden rush of power as you connect a jumper or install a card may damage sensitive electronic components.

Contents

CHAPTER 1

Overview

Sections include:

- Introduction
- Features
- Specifications
- Packing List
- Safety Precaution

Chapter 1 Overview

1.1 Introduction

To create reliability in your network, the EKI-7758F comes equipped with a proprietary redundant network protocol—X-Ring that was developed by Advantech, which provides users with an easy way to establish a redundant Ethernet network with ultra high-speed recovery time less than 10 ms.

Aside from 4 x 10/100/1000Base-T(X) fast Ethernet ports, the EKI-7758F come equipped with 4 SFP (mini-GBIC) fiber optic ports. Traditional RJ-45 ports can be used for uplinking wide-band paths in short distance (< 100 m), while the SFP slots can be used for the application of wideband uploading and long distance transmissions to fit the field request flexibility. Also, the long MTBF (Mean Time Between Failures) ensures that the EKI-7758F will continue to operate until a Gigabit network infrastructure has been established, without requiring any extra upgrade costs.

1.1.1 The SFP Advantage

The EKI-7758F's four SFP fiber slots provide a lot of flexibility when planning and implementing a network. The slots can accept any SFP-type fiber module and these modules are designed for transmitting over distances of either 500m (multi-mode), 10km, 30km, 50km, 70km or 110km (single-mode) – and the slots support SFP modules for WDM single-fiber transmissions. This means that you can easily change the transmission mode and distance of the switch by simply pulling out the SFP module and plugging in a different module. The SFP modules are hot-swappable and plug-and-play! Also, the fact that the switch has four of these slots, means that the network manager can, for example, have one 10km module in one slot and one 110km in the other.

1.1.2 High-Speed Transmissions

The EKI-7758F includes a switch controller that can automatically sense transmission speeds (10/100 Mbps). The RJ-45 interface can also be auto-detected, so MDI or MDI-X is automatically selected and a crossover cable is not required. All Ethernet ports have memory buffers that support the store-and-forward mechanism. This assures that data is properly transmitted.

1.1.3 Dual Power Input

To reduce the risk of power failure, the EKI-7758C provides +12 ~ 48 V_{DC} dual power inputs. with power reserve protection, which can prevent the switch device broken by wrong power wiring. When one of power input is fail, P-Fail LED will turn on and send an alarm through a relay output for notifying user.

1.1.4 Flexible Mounting

EKI-7758F is compact and can be mounted on a DIN-rail or panel, so it is suitable for any space-constrained environment.

1.1.5 Advanced Protection

The power line of EKI-7758F supports up to 3,000 V_{DC} EFT protection, which secure equipment against unregulated voltage and make systems safer and more reliable. Meanwhile, 4,000 V_{DC} ESD protections for Ethernet ports make EKI-7758F more suitable for harsh environments.

1.1.6 Wide Operating Temperature

The operating temperature of the EKI-7758F is between -10 ~ 60 ℃. With such a wide range, you can use the EKI-7758F in some of the harshest industrial environments that exist.

1.1.7 Easy Troubleshooting

LED indicators make troubleshooting quick and easy. Each 10/100/1000 Base-TX port has 2 LEDs that display the link status, transmission speed and collision status. Also the three power indicators P1, P2 and P-Fail help you diagnose immediately.

1.2 Features

- All Gigabit Ethernet ports for 4 Copper and 4 SFP
- SFP sockets for easy and flexible fiber expansion
- Redundancy: Gigabit X-Ring (ultra high-speed recovery time < 10ms), RSTP/STP (802.1w/1D)
- Management: Web, Telnet, Serial Console, Windows Utility, SNMP
- Control: VLAN/GVRP, QoS, IGMP Snooping, LACP, Rate Limit
- Security: IP/MAC and port binding, DHCP Server, IP access list, 802.1x, SNMPv3
- Diagnostic: Port statistic, Port Mirroring, RMON, Trap, SMTP Alert, Syslog
- Dual 12 ~ 48 V_{DC} power input and 1 Relay Output
- Robust mechanism and special heat spreader design

1.3 Specification

Communications

Standard	IEEE 802.3, 802.3ab, 802.3ad, 802.3u, 802.3x, 802.3z IEEE 802.1d, 802.1p, 802.1Q, 802.1w, 802.1X,
LAN	10/100/1000Base-TX, Optional 100Base-FX, 1000Base-SX/LX/LHX/XD/ZX/EZX
Transmission Distance	Ethernet: Up to 100m (4-wire Cat.5e, Cat.6 RJ-45 cable suggested for Gigabit port) SFP: Up to 110km (depends on SFP)
Transmission Speed	Gigabit Copper: 10/100/1000 Mbps, Auto-Negotiation Gigabit Fiber: Up to 1000Mbps

Interface

Connectors	4 x RJ-45 (Ethernet) 4 x SFP (mini-GBIC) ports 6-pin removable screw terminal (Power & Relay)
LED Indicators	System: PWR, R.M., PWR1, PWR2, P-Fail Gigabit Copper: Link/Activity, Speed (1000Mbps) SFP: Link/Activity
Console	RS-232 (RJ-45)

Network Management

Configuration	Web browser, Telnet, Serial Console, Windows Utility, TFTP, SNMP v1/v2c/v3, Port Speed/Duplex Configuration
VLAN	IEEE 802.1Q, GVRP, Port-based, VLAN
Redundancy	ADVANTECH X-Ring (Recovery time < 10ms at 30pcs full loading ring structure), Dual Homing, Couple Ring, 802.1w/D RSTP/STP
Security	IP Access security, post security, DHCP Server, Port and IP Binding, 802.1X Port Access Control
Traffic Control	IGMP Snooping/Query for multicast group management Port Trunking, Static/802.3ad LACP Rate limit and storm control IEEE 802.1p QoS Cos/TOS/DSCP priority queuing IEEE 802.3x flow control
Diagnostics	Port Mirroring, Real-time traffic statistic, MAC Address Table, SNTP, Syslog, E-Mail Alert, SNMP, Trap, RMON

Power

Power Consumption	Max. 17 W
Power Input	2 x Unregulated +12 ~ 48 V_{DC}
Fault Output	1 Relay Output

Mechanism

Dimensions (WxHxD)	79 x 152 x 105 mm
Enclosure	IP30, metal shell with solid mounting kits
Mounting	DIN-rail, wall

Protection

ESD (Ethernet)	4,000 V_{DC}
Surge (EFT for power)	3,000 V_{DC}
Power Reverse	Present
Overload	3.2A / 60V Replaceable Fuse

Environment

Operating Temperature	-10 ~ 60 ℃ (14 ~ 140 ℉)
Operating Humidity	5 ~ 95% (non-condensing)
Storage Temperature	-40 ~ 85 ℃ (-40~185 ℉)
Storage Humidity	0 ~ 95% (non-condensing)
MTBF	289,774 hours

Certifications

Safety	UL, 60950-1, CAN/CSA-C22.2 No.60950
EMC	U.S.A.: FCC Part 15 CISPR 22 EU: EN55011, EN61000-6-4 EN55022, Class A, EN61000-3-2/3 EN55024 IEC61000-4-2/3/4/5/6/8/11/12 EN61000-6-2
Freefall	IEC60068-2-32
Shock	IEC60068-2-27
Vibration	IEC60068-2-6

1.4 Packing List

- 1 x EKI-7758F Industrial Managed Gigabit Ethernet Switch
- 1 x eAutomation Industrial Communication CD-ROM with software, and User manual
- 2 x Wall Mounting Bracket and Screws
- 1 x DIN-rail Mounting Bracket and Screws
- 1 x 8-pin RJ-45 to RS-232 serial cable
- 1 x DC Jack Cable φ 2.0/150mm
- 1 x EKI-7758F Startup Manual

1.5 Safety Precaution

Attention *IF DC voltage is supplied by an external circuit, please use a protection device on the power supply input.*

CHAPTER 2

Installation

Sections include:

- LED Indicators
- Dimensions
- Mounting
- Network Connection
- Connection to a Fiber Optic Network
- Power Connection

Chapter 2 Installation

In this chapter, you will be given an overview of the EKI-7758F hardware installation procedures.

2.1 LED Indicators

There are few LEDs display the power status and network status located on the front panel of EKI-7758F, each of them has its own specific meaning shown as below.

Table 2.1: EKI-7758F LED Definition

LED	Color	Description	
PWR	Green	On	System power on
		Off	No power input
R.M.	Green	On	The industrial switch is the master of the X-ring group
		Off	The industrial switch is not the master of the X-ring group
PWR1	Green	On	Power input 1 is active
		Off	Power input 1 is inactive
PWR2	Green	On	Power input 2 is active
		Off	Power input 2 is inactive
P-Fail	Red	On	Power input 1 or 2 is inactive or port link down (depends on Fault Relay Alarm configuration)
		Off	Power input 1 and 2 are both active, or no power input
Link/Active (G5 ~ G8)	Green	On	SFP port is linking
		Flashing	Data is transmitting or receiving
		Off	Not connected to network
G1 ~ G4	Green (Upper LED)	On	Connected to network
		Flashing	Networking is active
		Off	Not connected to network
	Green (Lower LED)	On	The port is operating at speed of 1000M
		Off	The port is disconnected or not operating at speed of 1000M

2.2 Dimensions (units: mm)

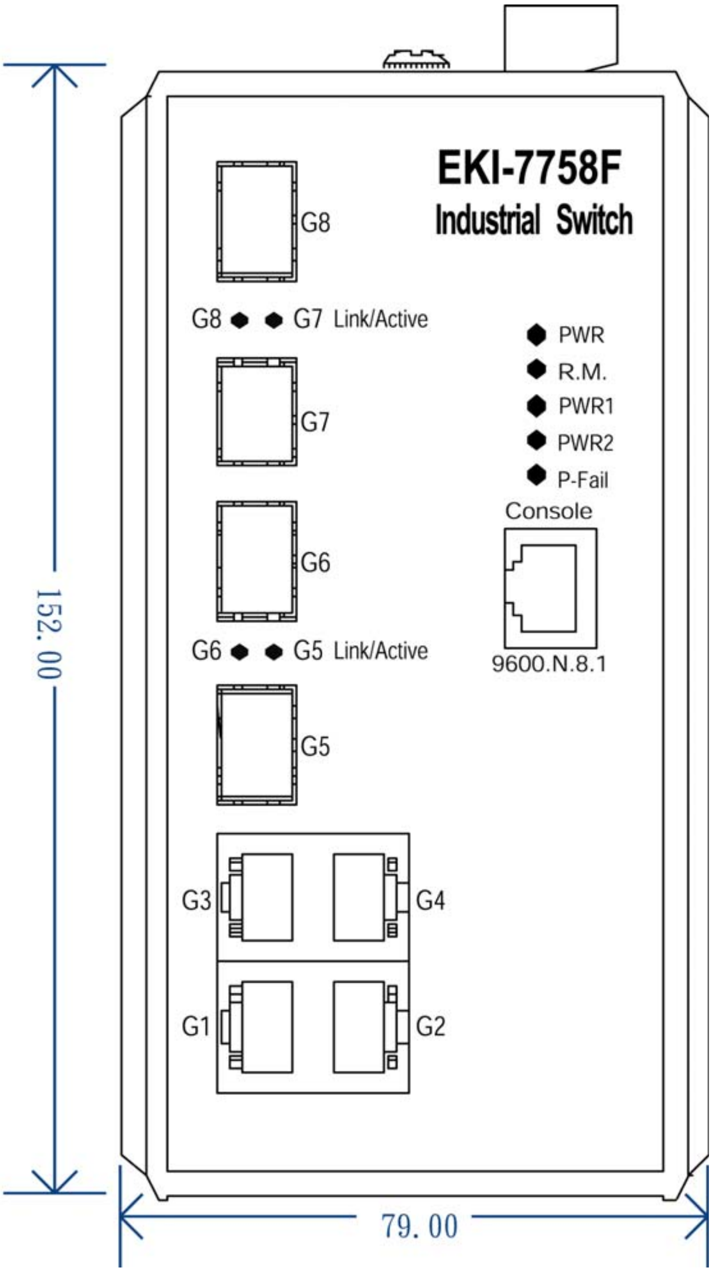


Figure 2.1: Front View of EKI-7758F

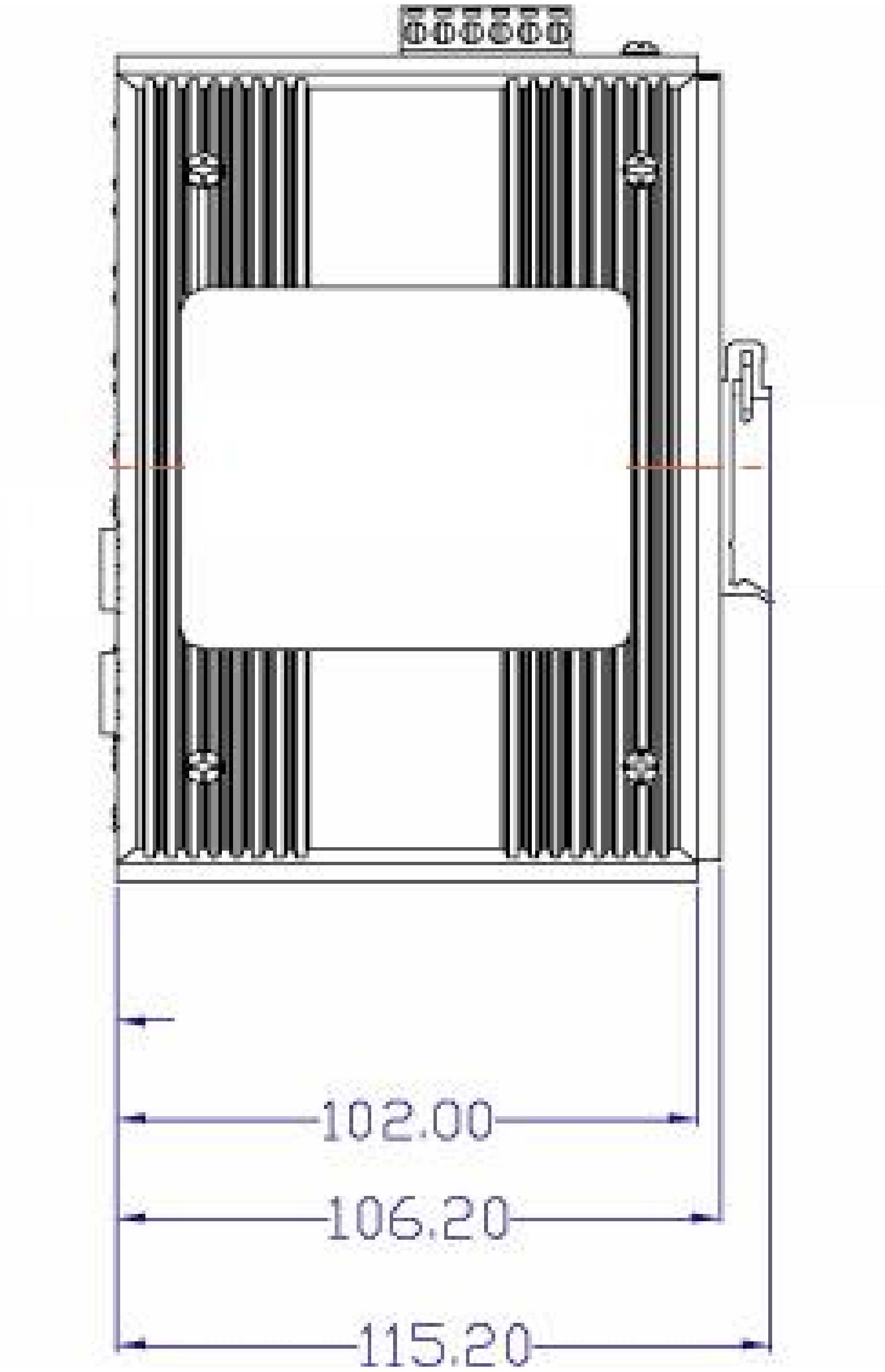


Figure 2.2: Side View of EKI-7758F

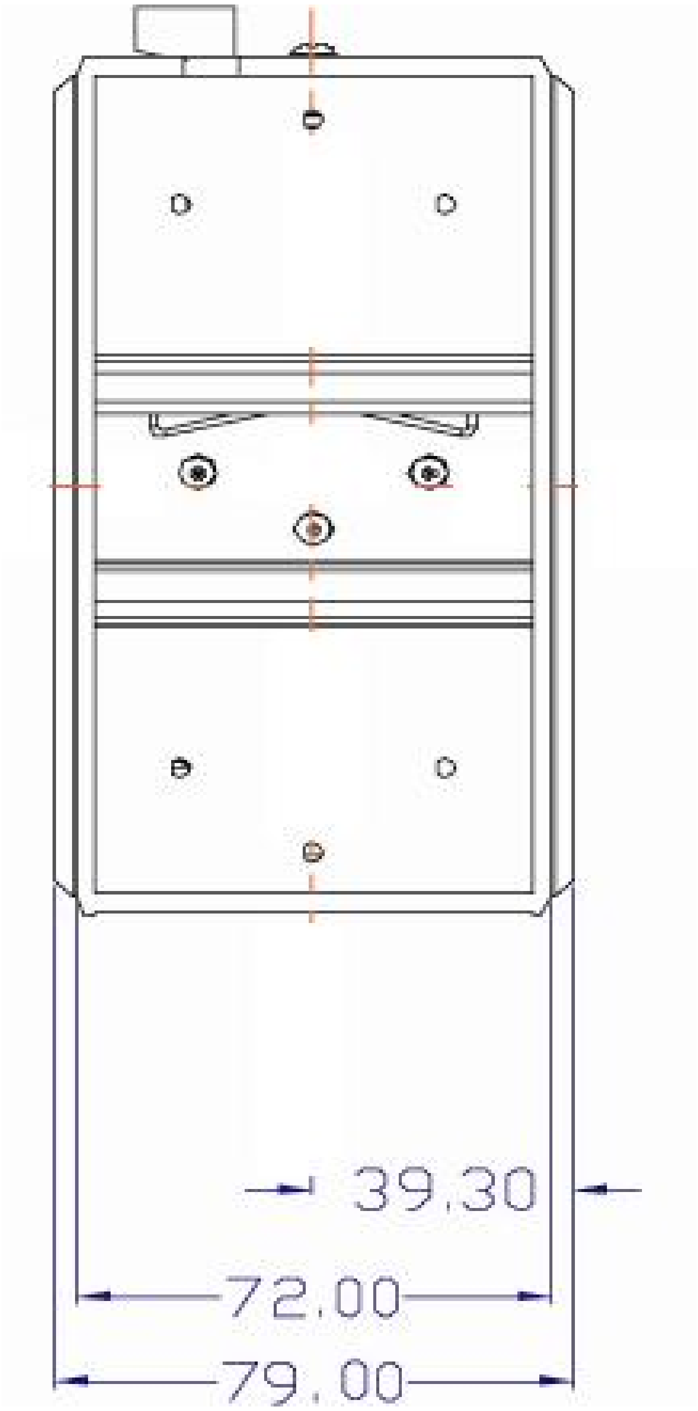


Figure 2.3: Rear View of EKI-7758F

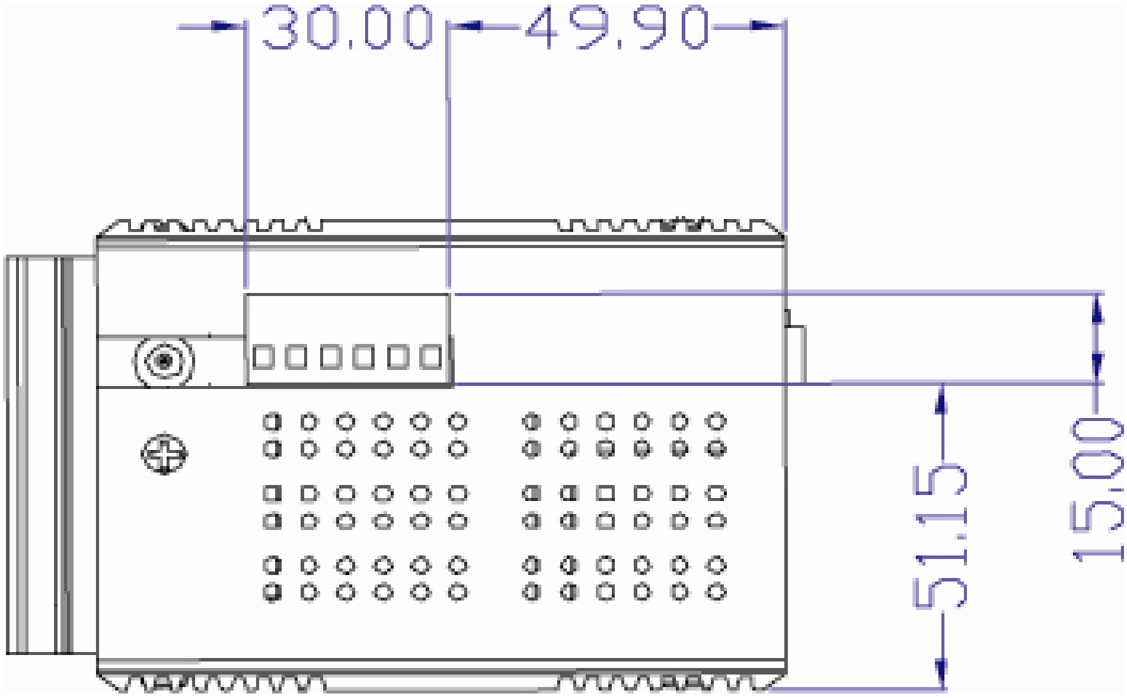


Figure 2.4: Top View of EKI-7758F

2.3 Mounting

The EKI-7758F supports two mounting methods: DIN-rail & Wall.

2.3.1 Wall mounting

EKI-7758F can be wall-mounted by using the included mounting kit. Then, hang on the EKI-7758F to the nails on the wall.
First, use the screws included in the package to combine the EKI-7758F and metal mounting kit. And then you can install the device firmly via the components, please see Figure 2.5 as below.

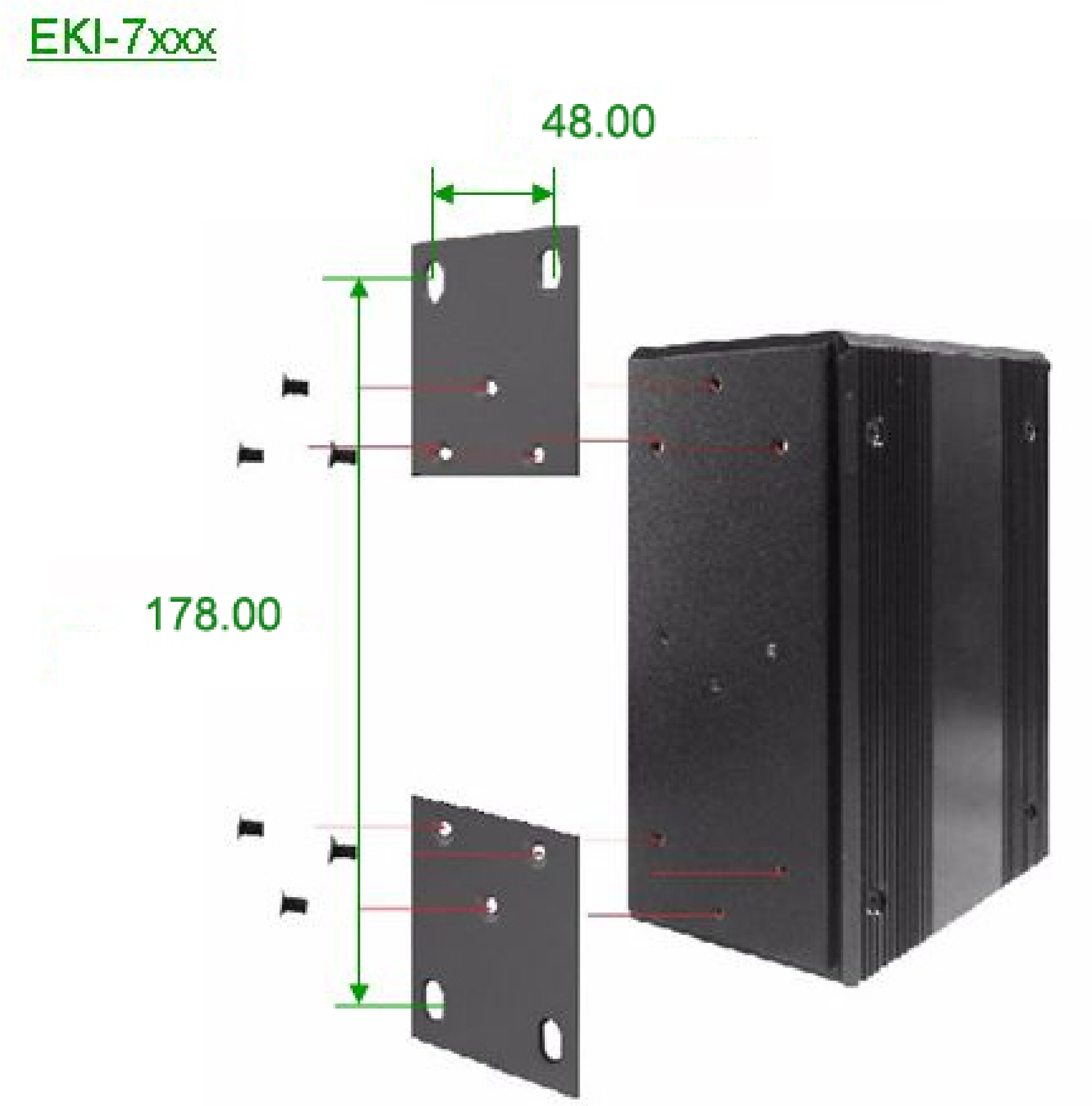


Figure 2.5: Combine the Metal Mounting Kit (units: mm)

2.3.2 DIN-rail Mounting

You can also mount EKI-7758F on a standard DIN-rail by below steps.

The DIN-rail kit is screwed on the industrial switch when out of factory. If the DIN-rail kit is not screwed on the industrial switch, please screw the DIN-rail kit on the switch first.

First, hang the EKI-7758F to the DIN-rail with angle of inclination. See Figure 2.6.

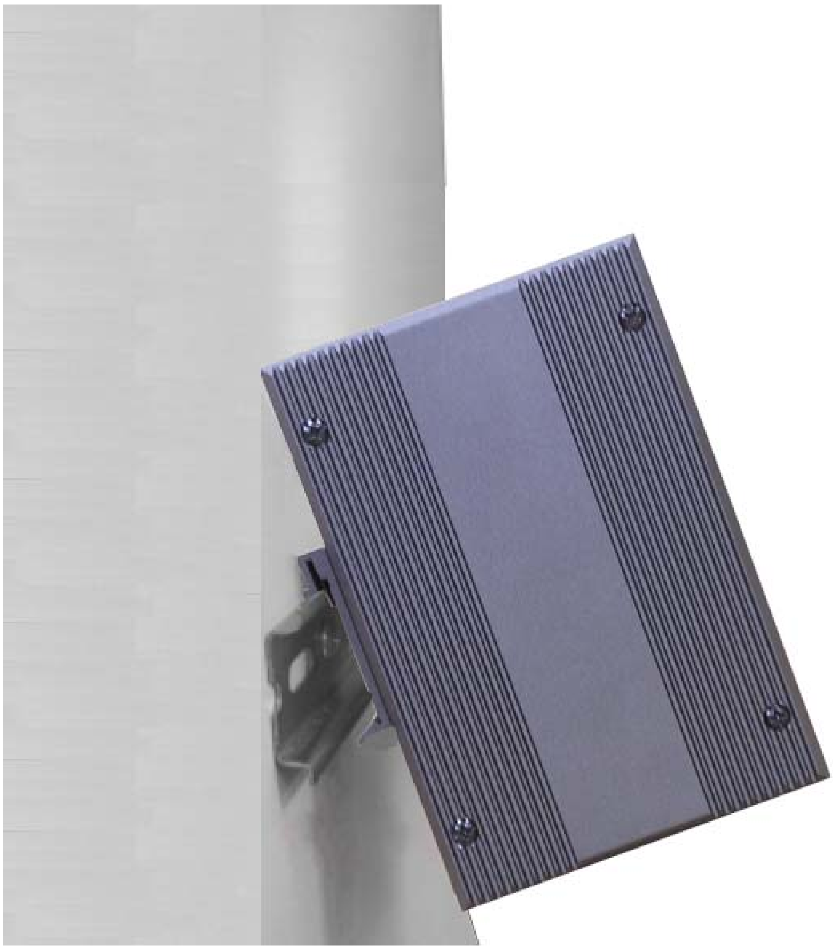


Figure 2.6: Installation to DIN-rail Step 1

Then, let the device down straight to slide over the rail smoothly. See Figure 2.7.

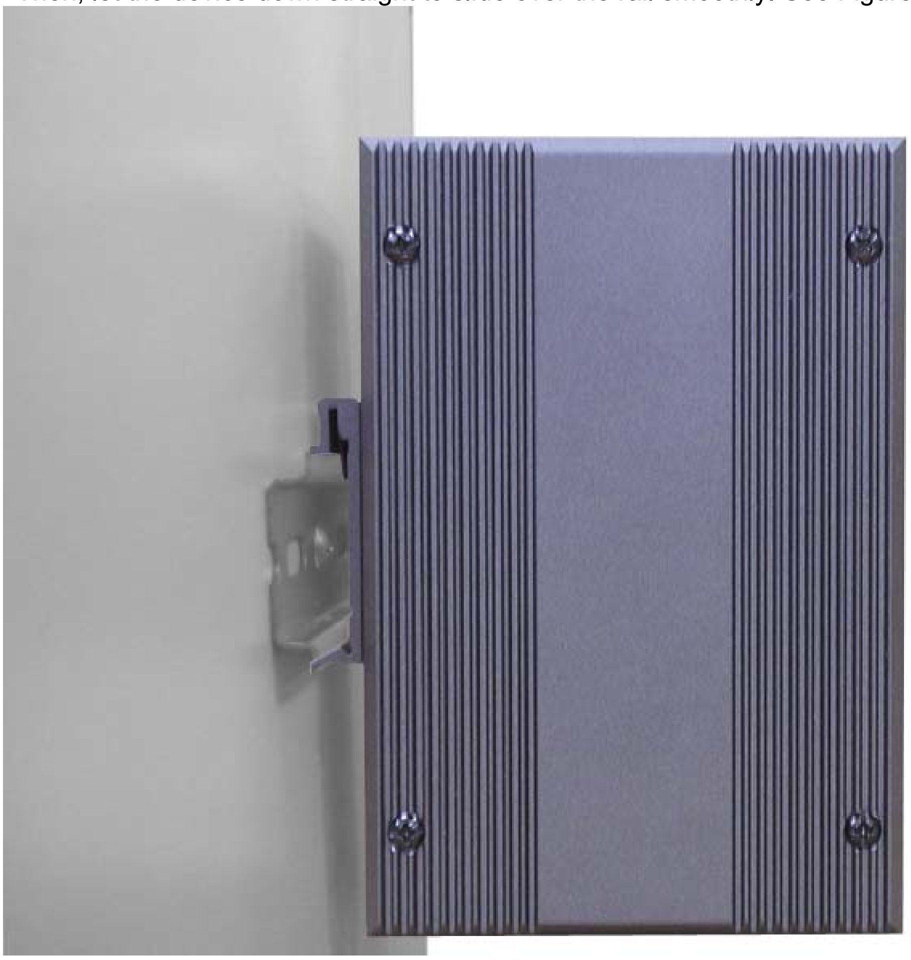


Figure 2.7: Installation to DIN-rail Step 2

2.4 Network Connection

The EKI-7758F has 4 x RJ-45 ports that support connection to 10 Mbps Ethernet, 100 Mbps Fast Ethernet or 1000 Mbps Gigabit Ethernet. EKI-7758F can be connected to other hubs or switches through a twisted-pair straight cable or a crossover cable up to 100m long. The connection can be made from any TX port of the EKI-7758F (MDI-X) to another hub or switch either MDI-X or uplink MDI port.

The EKI-7758F supports auto-crossover to make networking more easy and flexible. You can connect any RJ-45 (MDI-X) station port on the switch to any device such as a switch, bridge or router.

2.5 Connection to a Fiber Optic Network

EKI-7758F has 4 SFP slots for connecting to the network segment with single or multi-mode fiber. You can choose appropriate mini-GBIC module to plug into the slot. Make sure the module is aligned correctly and then slide the module into the SFP slot until a click is heard. You can use proper multi-mode or single-mode fiber according to the used SFP module. With fiber optic, it transmits speed up to 1000 Mbps and you can prevent noise interference from the system and transmission distance up to 110 km, depending on the mini-GBIC module.

- The small form-factor pluggable (SFP) is a compact optical transceiver used in optical communications for both telecommunication and data communications applications.

To connect the transceiver and LC cable, please follow the steps shown below:

First, insert the transceiver into the SFP module. Notice that the triangle mark is the bottom of the module.

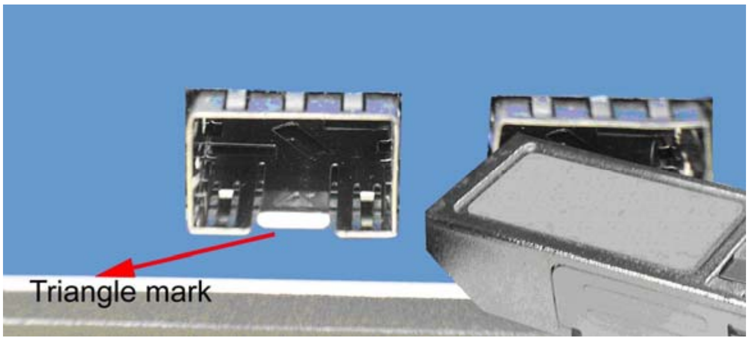


Figure 2.8: Transceiver to the SFP module

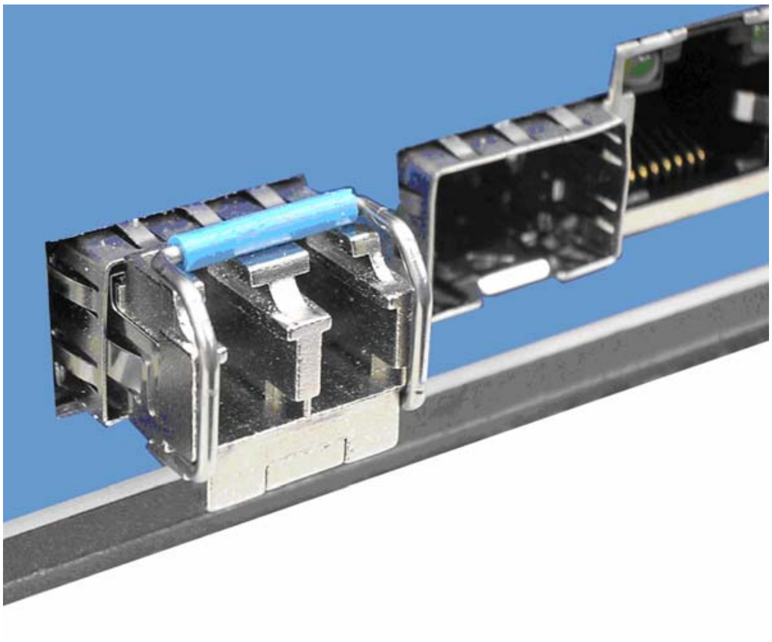


Figure 2.9: Transceiver Inserted

Second, insert the fiber cable of LC connector into the transceiver.

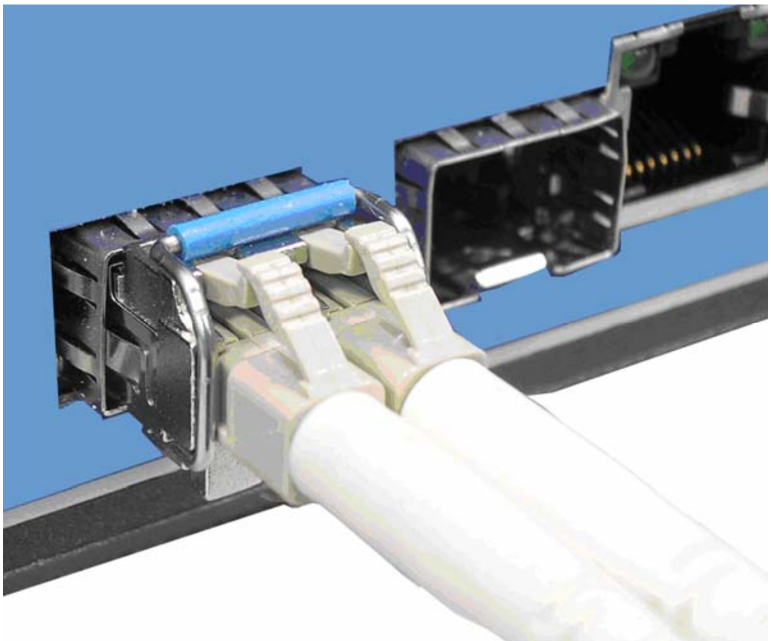


Figure 2.10: LC connector to the transceiver

To remove the LC connector from the transceiver, please follow the steps shown below:

First, press the upper side of the LC connector to release from the transceiver and pull it out.

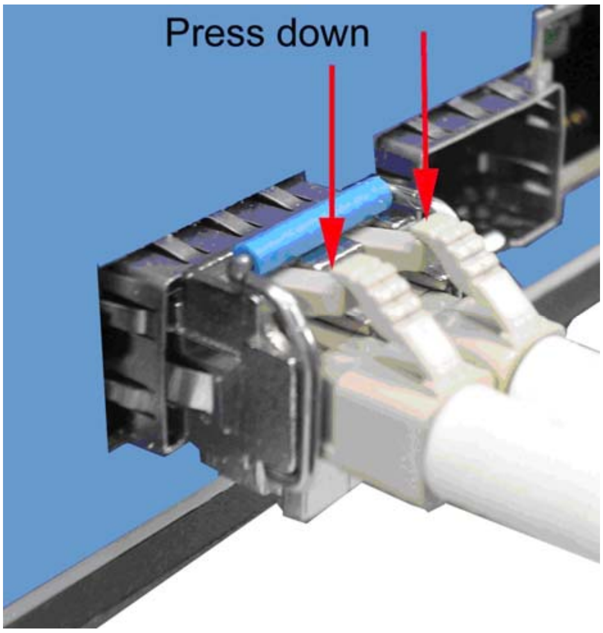


Figure 2.11: Remove LC connector

Second, push down the metal loop and pull the transceiver out by the plastic handle.

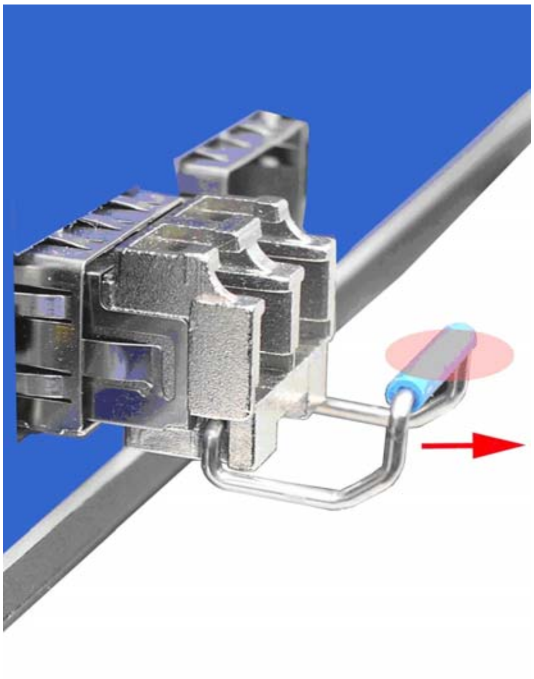


Figure 2.12: Pull out from the transceiver

2.6 Power Connection

The EKI-7758F supports dual +12 ~ 48 V_{DC} power inputs and power-fail relay output.

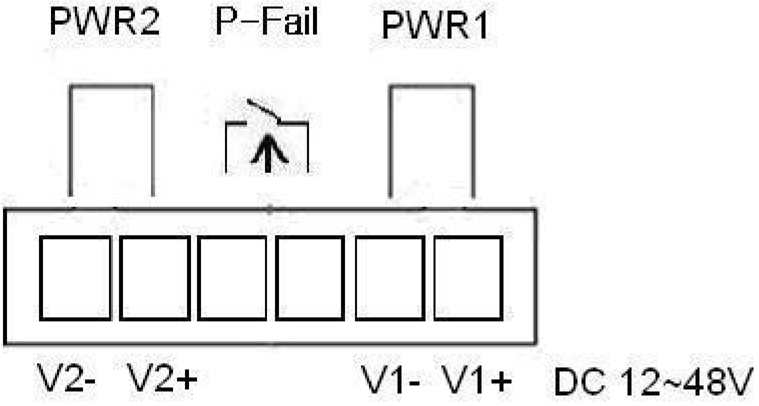


Figure 2.8: Pin Assignment of the Power Connector

You can connect an alarm indicator, buzzer or other signaling equipment through the relay output. The relay opens if power input 1, 2 fails or port link down/break (″Open″ means if you connect relay output with an LED, the light would be off).

CHAPTER 3

Configuration

Sections include:

- RS-232 Console
- Web Browser
- Mounting
- Self Diagnosis

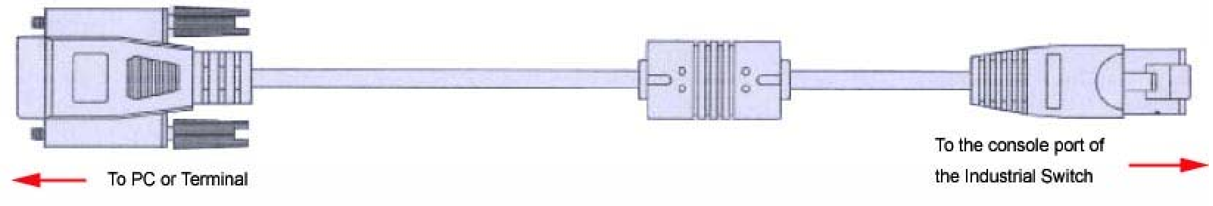
Chapter 3 Configuration

The EKI-7758F can be configured in two ways: via RS-232 Console or a web browser.

3.1 RS-232 Console

EKI-7758F's RS-232 console is designed for rapidly configuring which provides the console management – CLI command.

Attach the supplied cable, which one end is RJ-45 and the other end is female DB9, to connect EKI-7758F and your host PC or terminal. The connected PC or terminal must support the terminal emulation program.



From the Windows desktop, click:
Start/Programs/Accessories/Communications/HyperTerminal
to open Hyper Terminal program.

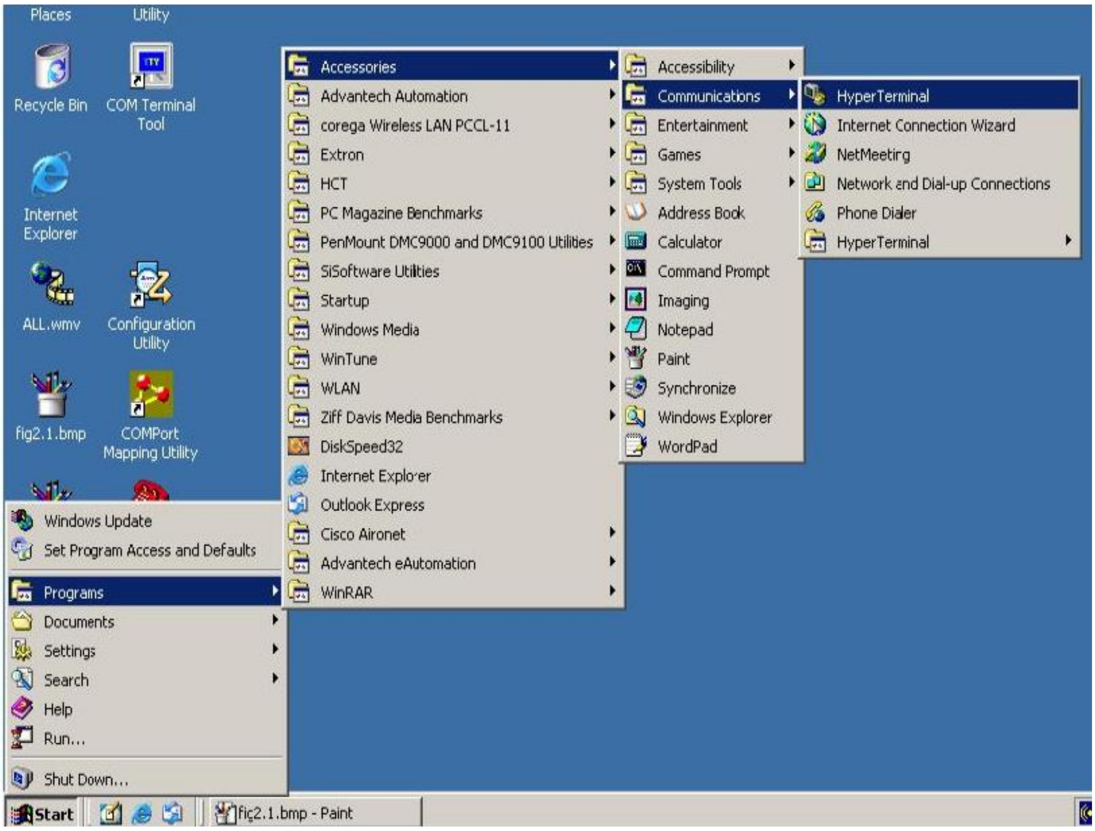
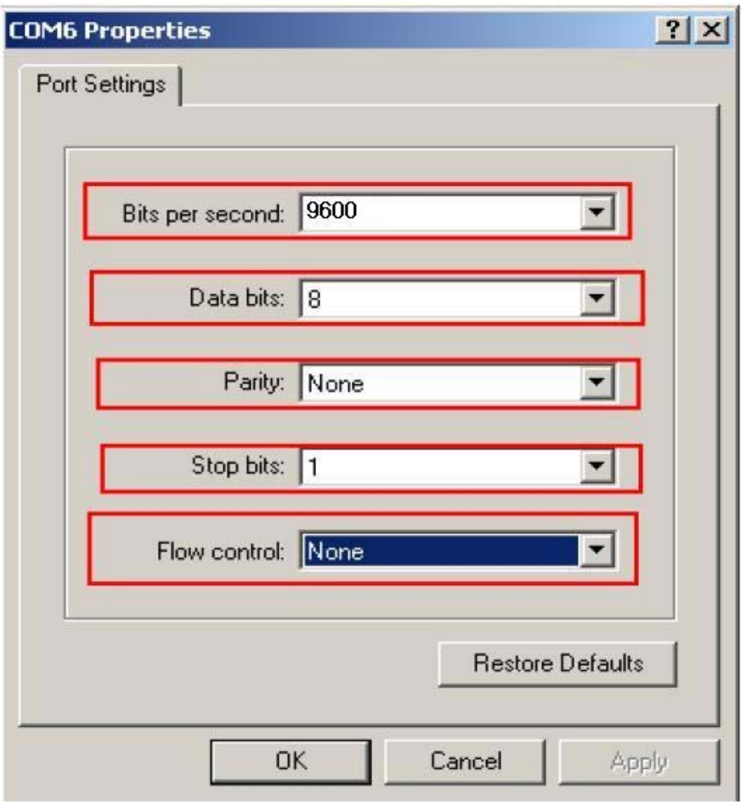


Figure 3.1: Open Hyper Terminal

Select the appropriate COM port, and set the parameter as Fig.3.2 (**9600** for **Baud Rate**, **8** for **Data Bits**, **None** for **Parity**, **1** for **Stop Bits**, and **None** for **Flow Control**).



COM6 Properties

Port Settings

Bits per second: 9600

Data bits: 8

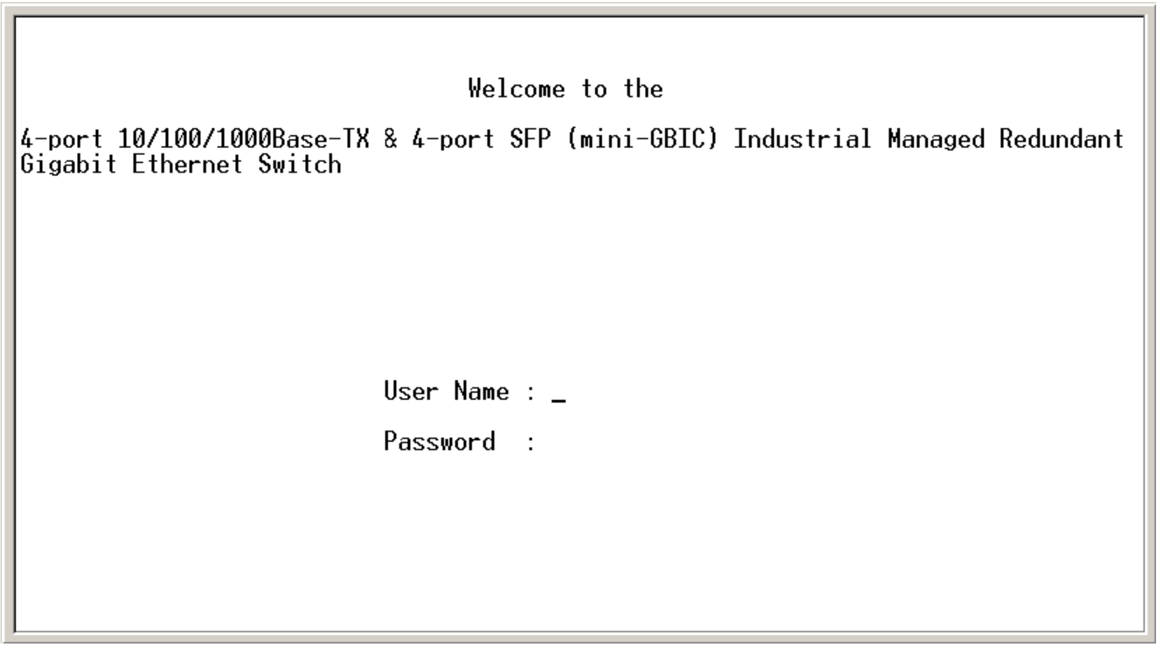
Parity: None

Stop bits: 1

Flow control: None

Figure 3.2: COM Port Properties Setting

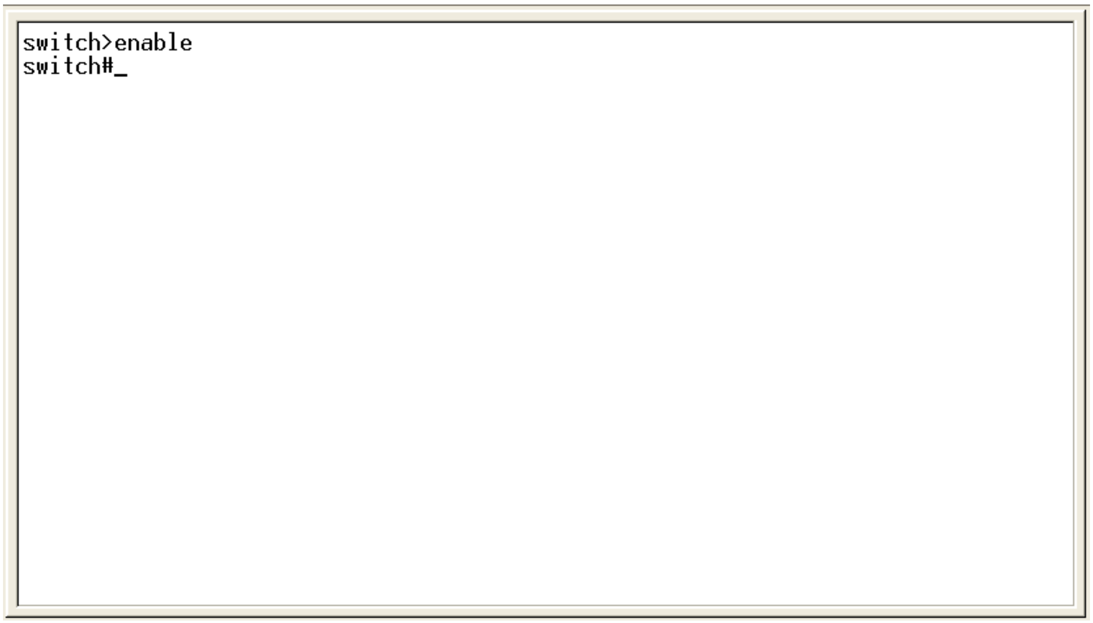
Press **Enter** for login screen (If you can not find the login screen, press **Enter** one more time). The default user name and password are both “**admin**”. Key-in the user name and password to enter the command line interface.



```
                           Welcome to the

4-port 10/100/1000Base-TX & 4-port SFP (mini-GBIC) Industrial Managed Redundant
Gigabit Ethernet Switch





                     User Name  : _

                     Password   :
```

Figure 3.3: Login Screen: RS-232 Configuration

After you have logged in to the system, you will see a command prompt. To enter CLI management interface, type in “**enable**” command.



```
switch>enable
switch#_
```

Figure 3.4: Command Line Interface

The following table lists the CLI commands and description.

3.1.1 Commands Level

Table 3.1: Command Level

Modes	Access Method	Prompt	Exit Method	About This Model
User EXEC	Begin a session with your switch.	switch>	Enter **logout** or **quit**.	The user commands available at the user level are a subset of those available at the privileged level. Use this mode to • Perform basic tests. • Display system information.
Privileged EXEC	Enter the **enable** command while in user EXEC mode.	switch#	Enter **disable** to exit.	The privileged command is advance mode Privileged this mode to • Display advance function status • save configures
Global configuration	Enter the **configure** command while in privileged EXEC mode.	switch(config)#	To exit to privileged EXEC mode, enter **exit** or **end**	Use this mode to configure parameters that apply to your switch as a whole.
VLAN database	Enter the **vlan database** command while in privileged EXEC mode.	switch(vlan)#	To exit to user EXEC mode, enter **exit**.	Use this mode to configure VLAN-specific parameters.
Interface configuration	Enter the **interface** command (with a specific interface) while in global configuration mode	switch(config-if)#	To exit to global configuration mode, enter **exit**. To exist to privileged EXEC mode, or **end.**	Use this mode to configure parameters for the switch and Ethernet ports.

3.1.2 Commands Set List

Table 3.2: Commands Set List

Command	Code Word
User EXEC	E
Privileged EXEC	P
Global configuration	G
VLAN database	V
Interface configuration	I

3.1.3 System Commands Set

Table 3.3: System Commands Set

Netstar Commands	Level	Description	Example
show config	E	Show switch configuration	switch>**show config**
show terminal	P	Show console information	switch#**show terminal**
write memory	P	Save user configuration into permanent memory (flash rom)	switch#**write memory**
system name [System Name]	G	Configure system name	switch(config)#**system name xxx**
system location [System Location]	G	Set switch system location string	switch(config)#**system location xxx**
system description [System Description]	G	Set switch system description string	switch(config)#**system description xxx**
system contact [System Contact]	G	Set switch system contact window string	switch(config)#**system contact xxx**
show system-info	E	Show system information	switch>**show system-info**
ip address [Ip-address] [Subnet-mask] [Gateway]	G	Configure the IP address of switch	switch(config)#**ip address 192.168.1.1 255.255.255.0 192.168.1.254**
ip dhcp	G	Enable DHCP client function of switch	switch(config)#**ip dhcp**
show ip	P	Show IP information of switch	switch#**show ip**
no ip dhcp	G	Disable DHCP client function of switch	switch(config)#**no ip dhcp**
reload	G	Halt and perform a cold restart	switch(config)#**reload**
default	G	Restore to default	switch(config)#**default**
admin username [Username]	G	Changes a login username. (maximum 10 words)	switch(config)#**admin username xxxxxx**
admin password [Password]	G	Specifies a password (maximum 10 words)	switch(config)#**admin password xxxxxx**
show admin	P	Show administrator information	switch#**show admin**
dhcpserver enable	G	Enable DHCP Server	switch(config)#**dhcpserver enable**
Dhcpserver disable	G	Disable DHCP Server	switch(config)#**no dhcpserver**
dhcpserver lowip [Low IP]	G	Configure low IP address for IP pool	switch(config)#**dhcpserver lowip 192.168.1.100**
dhcpserver highip [High IP]	G	Configure high IP address for IP pool	switch(config)#**dhcpserver highip 192.168.1.200**

dhcpserver subnetmask **[Subnet mask]**	**G**	Configure subnet mask for DHCP clients	switch(config)#**dhcpserver subnetmask 255.255.255.0**
dhcpserver gateway **[Gateway]**	**G**	Configure gateway for DHCP clients	switch(config)#**dhcpserver gateway 192.168.1.254**
dhcpserver dnsip **[DNS IP]**	**G**	Configure DNS IP for DHCP clients	switch(config)#**dhcpserver dnsip 192.168.1.1**
dhcpserver leasetime **[Hours]**	**G**	Configure lease time (in hour)	switch(config)#**dhcpserver leasetime 1**
dhcpserver ipbinding **[IP address]**	**I**	Set static IP for DHCP clients by port	switch(config)#**interface fastEthernet 2** switch(config)#**dhcpserver ipbinding 192.168.1.1**
show dhcpserver configuration	**P**	Show configuration of DHCP server	switch#**show dhcpserver configuration**
show dhcpserver clients	**P**	Show client entries of DHCP server	switch#**show dhcpserver clients**
show dhcpserver ip-binding	**P**	Show IP-Binding information of DHCP server	switch#**show dhcpserver ip-binding**
no dhcpserver	**G**	Disable DHCP server function	switch(config)#**no dhcpserver**
security enable	**G**	Enable IP security function	switch(config)#**security enable**
security http	**G**	Enable IP security of HTTP server	switch(config)#**security http**
security telnet	**G**	Enable IP security of telnet server	switch(config)#**security telnet**
security ip **[Index(1..10)] [IP Address]**	**G**	Set the IP security list	switch(config)#**security ip 1 192.168.1.55**
show security	**P**	Show the information of IP security	switch#**show security**
no security	**G**	Disable IP security function	switch(config)#**no security**
no security http	**G**	Disable IP security of HTTP server	switch(config)#**no security http**
no security telnet	**G**	Disable IP security of telnet server	switch(config)#**no security telnet**

3.1.4 Port Commands Set

Table 3.4: Port Commands Set

Netstar Commands	Level	Description	Example
interface fastEthernet [Portid]	**G**	Choose the port for modification.	switch(config)#**interface fastEthernet 2**
duplex [full | half]	**I**	Use the duplex configuration command to specify the duplex mode of operation for Fast Ethernet.	switch(config)#**interface fastEthernet 2** switch(config-if)#**duplex full**
speed [10|100|1000|auto]	**I**	Use the speed configuration command to specify the speed mode of operation for Fast Ethernet., the speed can't be set to 1000 if the port isn't a giga port..	switch(config)#**interface fastEthernet 2** switch(config-if)#**speed 100**
no flowcontrol	**I**	Disable flow control of interface	switch(config-if)#**no flowcontrol**
security enable	**I**	Enable security of interface	switch(config)#**interface fastEthernet 2** switch(config-if)#**security enable**
no security	**I**	Disable security of interface	switch(config)#**interface fastEthernet 2** switch(config-if)#**no security**

bandwidth type all	I	Set interface ingress limit frame type to "accept all frame"	switch(config)#**interface fastEthernet 2** switch(config-if)#**bandwidth type all**
bandwidth type broadcast-multicast-flooded-unicast	I	Set interface ingress limit frame type to "accept broadcast, multicast, and flooded unicast frame"	switch(config)#**interface fastEthernet 2** switch(config-if)#**bandwidth type broadcast-multicast-flooded-unicast**
bandwidth type broadcast-multicast	I	Set interface ingress limit frame type to "accept broadcast and multicast frame"	switch(config)#**interface fastEthernet 2** switch(config-if)#**bandwidth type broadcast-multicast**
bandwidth type broadcast-only	I	Set interface ingress limit frame type to "only accept broadcast frame"	switch(config)#**interface fastEthernet 2** switch(config-if)#**bandwidth type broadcast-only**
bandwidth in [Value]	I	Set interface input bandwidth. Rate Range is from 100 kbps to 102400 kbps or to 256000 kbps for giga ports, and zero means no limit.	switch(config)#**interface fastEthernet 2** switch(config-if)#**bandwidth in 100**
bandwidth out [Value]		Set interface output bandwidth. Rate Range is from 100 kbps to 102400 kbps or to 256000 kbps for giga ports, and zero means no limit.	switch(config)#**interface fastEthernet 2** switch(config-if)#**bandwidth out 100**
show bandwidth	I	Show interfaces bandwidth control	switch(config)#**interface fastEthernet 2** switch(config-if)#**show bandwidth**
state [Enable | Disable]	I	Use the state interface configuration command to specify the state mode of operation for Ethernet ports. Use the disable form of this command to disable the port.	switch(config)#**interface fastEthernet 2** switch(config-if)#**state Disable**
show interface configuration	I	show interface configuration status	switch(config)#**interface fastEthernet 2** switch(config-if)#**show interface configuration**
show interface status	I	show interface actual status	switch(config)#**interface fastEthernet 2** switch(config-if)#**show interface status**
show interface accounting	I	show interface statistic counter	switch(config)#**interface fastEthernet 2** switch(config-if)#**show interface accounting**
no accounting	I	Clear interface accounting information	switch(config)#**interface fastEthernet 2** switch(config-if)#**no accounting**

3.1.5 Trunk Commands Set

Table 3.5: Trunk Commands Set

Netstar Commands	Level	Description	Example
aggregator priority [1~65535]	G	Set port group system priority	switch(config)#**aggregator priority 22**
aggregator activityport [Group ID] [Port Numbers]	G	Set activity port	switch(config)#**aggregator activityport 2**
aggregator group [GroupID] [Port-list] **lacp** **workp** [Workport]	G	Assign a trunk group with LACP active. [GroupID] :1~3 [Port-list]:Member port list, This parameter could be a port range(ex.1-4) or a port list separate by a comma(ex.2, 3, 6) [Workport]: The amount of work ports, this value could not be less than zero or be large than the amount of member ports.	switch(config)#**aggregator group 1 1-4 lacp workp 2** or switch(config)#**aggregator group 2 1,4,3 lacp workp 3**

aggregator group [GroupID] [Port-list] **nolacp**	G	Assign a static trunk group. [GroupID] :1~3 [Port-list]:Member port list, This parameter could be a port range(ex.1-4) or a port list separate by a comma(ex.2, 3, 6)	switch(config)#**aggregator group 1 2-4 nolacp** or switch(config)#**aggregator group 1 3,1,2 nolacp**
show aggregator	P	Show the information of trunk group	switch#**show aggregator 1** or switch#**show aggregator 2** or switch#**show aggregator 3**
no aggregator lacp [GroupID]	G	Disable the LACP function of trunk group	switch(config)#**no aggreator lacp 1**
no aggregator group [GroupID]	G	Remove a trunk group	switch(config)#**no aggreator group 2**

3.1.6 VLAN Commands Set

Table 3.6: VLAN Commands Set

Netstar Commands	Level	Description	Example
vlan database	P	Enter VLAN configure mode	switch#**vlan database**
Vlanmode [portbase| 802.1q | gvrp]	V	To set switch VLAN mode.	switch(vlan)#**vlanmode portbase** or switch(vlan)#**vlanmode 802.1q** or switch(vlan)#**vlanmode gvrp**
no vlan	V	No VLAN	Switch(vlan)#**no vlan**
Ported based VLAN configuration			
vlan port-based grpname [Group Name] **grpid** [GroupID] **port** [PortNumbers]	V	Add new port based VALN	switch(vlan)#**vlan port-based grpname test grpid 2 port 2-4** or switch(vlan)#**vlan port-based grpname test grpid 2 port 2,3,4**
show vlan [GroupID] or **show vlan**	V	Show VLAN information	switch(vlan)#**show vlan 23**
no vlan group [GroupID]	V	Delete port base group ID	switch(vlan)#**no vlan group 2**
IEEE 802.1Q VLAN			
vlan 8021q name [GroupName] **vid** [VID]	V	Change the name of VLAN group, if the group didn't exist, this command can't be applied.	switch(vlan)#**vlan 8021q name test vid 22**
vlan 8021q port [PortNumber] **access-link untag** [UntaggedVID]	V	Assign a access link for VLAN by port, if the port belong to a trunk group, this command can't be applied.	switch(vlan)#**vlan 8021q port 3 access-link untag 33**
vlan 8021q port [PortNumber] **trunk-link tag** [TaggedVID List]	V	Assign a trunk link for VLAN by port, if the port belong to a trunk group, this command can't be applied.	switch(vlan)#**vlan 8021q port 3 trunk-link tag 2,3,6,99** or switch(vlan)#**vlan 8021q port 3 trunk-link tag 3-20**
vlan 8021q port [PortNumber] **hybrid-link untag** [UntaggedVID] **tag** [TaggedVID List]	V	Assign a hybrid link for VLAN by port, if the port belong to a trunk group, this command can't be applied.	switch(vlan)#**vlan 8021q port 3 hybrid-link untag 4 tag 3,6,8** or switch(vlan)#**vlan 8021q port 3 hybrid-link untag 5 tag 6-8**

vlan 8021q trunk [PortNumber] **access-link untag** [UntaggedVID]	V	Assign a access link for VLAN by trunk group	switch(vlan)#**vlan 8021q trunk 3 access-link untag 33**
vlan 8021q trunk [PortNumber] **trunk-link tag** [TaggedVID List]	V	Assign a trunk link for VLAN by trunk group	switch(vlan)#**vlan 8021q trunk 3 trunk-link tag 2,3,6,99** or switch(vlan)#**vlan 8021q trunk 3 trunk-link tag 3-20**
vlan 8021q trunk [PortNumber] **hybrid-link untag** [UntaggedVID] **tag** [TaggedVID List]	V	Assign a hybrid link for VLAN by trunk group	switch(vlan)#**vlan 8021q trunk 3 hybrid-link untag 4 tag 3,6,8** or switch(vlan)#**vlan 8021q trunk 3 hybrid-link untag 5 tag 6-8**
show vlan [GroupID] or **show vlan**	V	Show VLAN information	switch(vlan)#**show vlan 23**
no vlan group [GroupID]	V	Delete port base group ID	switch(vlan)#**no vlan group 2**

3.1.7 Spanning Tree Commands Set

Table 3.7: Spanning Tree Commands Set

Netstar Commands	Level	Description	Example
spanning-tree enable	G	Enable spanning tree	switch(config)#**spanning-tree enable**
spanning-tree priority [0~61440]	G	Configure spanning tree priority parameter	switch(config)#**spanning-tree priority 32767**
spanning-tree max-age [seconds]	G	Use the spanning-tree max-age global configuration command to change the interval between messages the spanning tree receives from the root switch. If a switch does not receive a bridge protocol data unit (BPDU) message from the root switch within this interval, it recomputed the Spanning Tree Protocol (STP) topology.	switch(config)#**spanning-tree max-age 15**
spanning-tree hello-time [seconds]	G	Use the spanning-tree hello-time global configuration command to specify the interval between hello bridge protocol data units (BPDUs).	switch(config)#**spanning-tree hello-time 3**
spanning-tree forward-time [seconds]	G	Use the spanning-tree forward-time global configuration command to set the forwarding-time for the specified spanning-tree instances. The forwarding time determines how long each of the listening and learning states last before the port begins forwarding.	switch(config)#**spanning-tree forward-time 20**
stp-path-cost [1~200000000]	I	Use the spanning-tree cost interface configuration command to set the path cost for Spanning Tree Protocol (STP) calculations. In the event of a loop, spanning tree considers the path cost when selecting an interface to place into the forwarding state.	switch(config)#**interface fastEthernet 2** switch(config-if)#**stp-path-cost 20**
stp-path-priority [Port Priority]	I	Use the spanning-tree port-priority interface configuration command to configure a port priority that is used when two switches tie for	switch(config)#**interface fastEthernet 2** switch(config-if)#**stp-path-priority 128**

		position as the root switch.	
stp-admin-p2p [Auto|True|False]	**I**	Admin P2P of STP priority on this interface.	switch(config)#**interface fastEthernet 2** switch(config-if)#**stp-admin-p2p Auto**
stp-admin-edge [True|False]	**I**	Admin Edge of STP priority on this interface.	switch(config)#**interface fastEthernet 2** switch(config-if)#**stp-admin-edge True**
stp-admin-non-stp [True|False]	**I**	Admin NonSTP of STP priority on this interface.	switch(config)#**interface fastEthernet 2** switch(config-if)#**stp-admin-non-stp False**
show spanning-tree	**E**	Displays a summary of the spanning-tree states.	switch>**show spanning-tree**
no spanning-tree	**G**	Disable spanning-tree.	switch(config)#**no spanning-tree**

3.1.8 QOS Commands Set

Table 3.8: QOS Commands Set

Netstar Commands	Level	Description	Example
qos policy [weighted-fair|strict]	**G**	Select QOS policy scheduling	switch(config)#**qos policy weighted-fair**
qos prioritytype [port-based|cos-only|tos-only|cos-first|tos-first]	**G**	Setting of QOS priority type	switch(config)#**qos prioritytype**
qos priority portbased [Port] [lowest|low|middle|high]	**G**	Configure Port-based Priority	switch(config)#**qos priority portbased 1 low**
qos priority cos [Priority][lowest|low|middle|high]	**G**	Configure COS Priority	switch(config)#**qos priority cos 0 middle**
qos priority tos [Priority][lowest|low|middle|high]	**G**	Configure TOS Priority	switch(config)#**qos priority tos 3 high**
show qos	**P**	Displays the information of QoS configuration	Switch#**show qos**
no qos	**G**	Disable QoS function	switch(config)#**no qos**

3.1.9 IGMP Commands Set

Table 3.9: QOS Commands Set

Netstar Commands	Level	Description	Example
igmp enable	**G**	Enable IGMP snooping function	switch(config)#**igmp enable**
Igmp-query auto	**G**	Set IGMP query to auto mode	switch(config)#**Igmp-query auto**
Igmp-query force	**G**	Set IGMP query to force mode	switch(config)#**Igmp-query force**
show igmp configuration	**P**	Displays the details of an IGMP configuration.	switch#**show igmp configuration**
show igmp multi	**P**	Displays the details of an IGMP snooping entries.	switch#**show igmp multi**
no igmp	**G**	Disable IGMP snooping function	switch(config)#**no igmp**
no igmp-query	**G**	Disable IGMP query	switch#**no igmp-query**

3.1.10 Mac/Filter Table Commands Set

Table 3.10: Mac/Filter Table Commands Set

Netstar Commands	Level	Description	Example
mac-address-table static hwaddr [MAC]	I	Configure MAC address table of interface (static).	switch(config)#**interface fastEthernet 2** switch(config-if)#**mac-address-table static hwaddr 000012345678**
mac-address-table filter hwaddr [MAC]	G	Configure MAC address table(filter)	switch(config)#**mac-address-table filter hwaddr 000012348678**
show mac-address-table	P	Show all MAC address table	switch#**show mac-address-table**
show mac-address-table static	P	Show static MAC address table	switch#**show mac-address-table static**
show mac-address-table filter	P	Show filter MAC address table.	switch#**show mac-address-table filter**
no mac-address-table static hwaddr [MAC]	I	Remove an entry of MAC address table of interface (static)	switch(config)#**interface fastEthernet 2** switch(config-if)#**no mac-address-table static hwaddr 000012345678**
no mac-address-table filter hwaddr [MAC]	G	Remove an entry of MAC address table (filter)	switch(config)#**no mac-address-table filter hwaddr 000012348678**
no mac-address-table	G	Remove dynamic entry of MAC address table	switch(config)#**no mac-address-table**

3.1.11 SNMP Commands Set

Table 3.11: SNMP Commands Set

Netstar Commands	Level	Description	Example
snmp system-name [System Name]	G	Set SNMP agent system name	switch(config)#**snmp system-name l2switch**
snmp system-location [System Location]	G	Set SNMP agent system location	switch(config)#**snmp system-location lab**
snmp system-contact [System Contact]	G	Set SNMP agent system contact	switch(config)#**snmp system-contact where**
snmp agent-mode [v1v2c|v3|v1v2cv3]	G	Select the agent mode of SNMP	switch(config)#**snmp agent-mode v1v2cv3**
snmp community-strings [Community] **right** [RO/RW]	G	Add SNMP community string.	switch(config)#**snmp community-strings public right rw**
snmp-server host [IP address] **community** [Community-string] **trap-version** [v1|v2c]	G	Configure SNMP server host information and community string	switch(config)#**snmp-server host 192.168.1.50 community public trap-version v1** **(remove)** Switch(config)# **no snmp-server host 192.168.1.50**
snmpv3 context-name [Context Name]	G	Configure the context name	switch(config)#**snmpv3 context-name Test**
snmpv3 user [User Name] **group** [Group Name] **password** [Authentication Password] [Privacy Password]	G	Configure the userprofile for SNMPV3 agent. Privacy password could be empty.	switch(config)#**snmpv3 user test01 group G1 password AuthPW PrivPW**
snmpv3 access context-name [Context Name] **group** [Group Name] **security-level** [NoAuthNoPriv|AuthNoPriv|AuthPriv] **match-rule** [Exact|Prifix] **views** [Read View Name] [Write View Name] [Notify View Name]	G	Configure the access table of SNMPV3 agent	switch(config)#**snmpv3 access context-name Test group G1 security-level AuthPriv match-rule Exact views V1 V1 V1**
snmpv3 mibview view [View Name] **type** [Excluded|Included]	G	Configure the mibview table of SNMPV3 agent	switch(config)#**snmpv3 mibview view V1 type Excluded sub-oid 1.3.6.1**

sub-oid [OID]			
show snmp	P	Show SNMP configuration	switch#**show snmp**
no snmp community-strings [Community]	G	Remove the specified community.	switch(config)#**no snmp community-strings public**
no snmp-server host [Host-address]	G	Remove the SNMP server host.	switch(config)#**no snmp-server 192.168.1.50**
no snmpv3 user [User Name]	G	Remove specified user of SNMPv3 agent.	switch(config)#**no snmpv3 user Test**
no snmpv3 access context-name [Context Name] **group** [Group Name] **security-level** [NoAuthNoPriv|AuthNoPriv|AuthPriv] **match-rule** [Exact|Prifix] **views** [Read View Name] [Write View Name] [Notify View Name]	G	Remove specified access table of SNMPv3 agent.	switch(config)#**no snmpv3 access context-name Test group G1 security-level AuthPr iv match-rule Exact views V1 V1 V1**
no snmpv3 mibview view [View Name] **type** [Excluded|Included] **sub-oid** [OID]	G	Remove specified mibview table of SNMPV3 agent.	switch(config)#**no snmpv3 mibview view V1 type Excluded sub-oid 1.3.6.1**

3.1.12 Port Mirroring Commands Set

Table 3.12: Port Mirroring Commands Set

Netstar Commands	Level	Description	Example
monitor rx	G	Set RX destination port of monitor function	switch(config)#**monitor rx**
monitor tx	G	Set TX destination port of monitor function	switch(config)#**monitor tx**
show monitor	P	Show port monitor information	switch#**show monitor**
monitor [RX|TX|Both]	I	Configure source port of monitor function	switch(config)#**interface fastEthernet 2** switch(config-if)#**monitor RX**
show monitor	I	Show port monitor information	switch(config)#**interface fastEthernet 2** switch(config-if)#**show monitor**
no monitor	I	Disable source port of monitor function	switch(config)#**interface fastEthernet 2** switch(config-if)#**no monitor**

3.1.13 802.1x Commands Set

Table 3.13: 802.1x Commands Set

Netstar Commands	Level	Description	Example
8021x enable	G	Use the 802.1x global configuration command to enable 802.1x protocols.	switch(config)# **8021x enable**
8021x system radiousip **[IP address]**	G	Use the 802.1x system radious IP global configuration command to change the radious server IP.	switch(config)# **8021x system radiousip 192.168.1.1**
8021x system serverport **[port ID]**	G	Use the 802.1x system server port global configuration command to	switch(config)# **8021x system serverport 1815**

		change the radious server port	
8021x system accountport **[port ID]**	**G**	Use the 802.1x system account port global configuration command to change the accounting port	switch(config)# **8021x system accountport 1816**
8021x system sharekey **[ID]**	**G**	Use the 802.1x system share key global configuration command to change the shared key value.	switch(config)# **8021x system sharekey 123456**
8021x system nasid **[words]**	**G**	Use the 802.1x system nasid global configuration command to change the NAS ID	switch(config)# **8021x system nasid test1**
8021x misc quietperiod **[sec.]**	**G**	Use the 802.1x misc quiet period global configuration command to specify the quiet period value of the switch.	switch(config)# **8021x misc quietperiod 10**
8021x misc txperiod **[sec.]**	**G**	Use the 802.1x misc TX period global configuration command to set the TX period.	switch(config)# **8021x misc txperiod 5**
8021x misc supportimeout [sec.]	**G**	Use the 802.1x misc supp timeout global configuration command to set the supplicant timeout.	switch(config)# **8021x misc supportimeout 20**
8021x misc servertimeout [sec.]	**G**	Use the 802.1x misc server timeout global configuration command to set the server timeout.	switch(config)#**8021x misc servertimeout 20**
8021x misc maxrequest [number]	**G**	Use the 802.1x misc max request global configuration command to set the MAX requests.	switch(config)# **8021x misc maxrequest 3**
8021x misc reauthperiod [sec.]	**G**	Use the 802.1x misc reauth period global configuration command to set the reauth period.	switch(config)# **8021x misc reauthperiod 3000**
8021x portstate **[disable | reject | accept | authorize]**	**I**	Use the 802.1x port state interface configuration command to set the state of the selected port.	switch(config)#**interface fastethernet 3** switch(config-if)#**8021x portstate accept**
show 8021x	**E**	Displays a summary of the 802.1x properties and also the port sates.	switch>**show 8021x**
no 8021x	**G**	Disable 802.1x function	switch(config)#**no 8021x**

3.1.14 TFTP Commands Set

Table 3.14: TFTP Commands Set

Netstar Commands	Level	Description	Defaults Example
backup flash:backup_cfg	**G**	Save configuration to TFTP and need to specify the IP of TFTP server and the file name of image.	switch(config)#**backup flash:backup_cfg**
restore flash:restore_cfg	**G**	Get configuration from TFTP server and need to specify the IP of TFTP server and the file name of image.	switch(config)#**restore flash:restore_cfg**
upgrade flash:upgrade_fw	**G**	Upgrade firmware by TFTP and need to specify the IP of TFTP server and the file name of image.	switch(config)#**upgrade lash:upgrade_fw**

3.1.15 SystemLog, SMTP and Event

Table 3.15: SysLog,SMTP,Event Commands Set

Netstar Commands	Level	Description	Example
systemlog ip [IP address]	**G**	Set System log server IP address.	switch(config)# **systemlog ip 192.168.1.100**

systemlog mode [client|server|both]	G	Specified the log mode	switch(config)# **systemlog mode both**
show systemlog	E	Displays system log.	Switch>**show systemlog**
show systemlog	P	Show system log client & server information	switch#**show systemlog**
no systemlog	G	Disable systemlog functon	switch(config)#**no systemlog**
smtp enable	G	Enable SMTP function	switch(config)#**smtp enable**
smtp serverip [IP address]	G	Configure SMTP server IP	switch(config)#**smtp serverip 192.168.1.5**
smtp authentication	G	Enable SMTP authentication	switch(config)#**smtp authentication**
smtp account [account]	G	Configure authentication account	switch(config)#**smtp account User**
smtp password [password]	G	Configure authentication password	switch(config)#**smtp password**
smtp rcptemail [Index] [Email address]	G	Configure Rcpt e-mail Address	switch(config)#**smtp rcptemail 1 Alert@test.com**
show smtp	P	Show the information of SMTP	switch#**show smtp**
no smtp	G	Disable SMTP function	switch(config)#**no smtp**
event device-cold-start **[Systemlog|SMTP|Both]**	G	Set cold start event type	switch(config)#**event device-cold-start both**
event authentication-failure [Systemlog|SMTP|Both]	G	Set Authentication failure event type	switch(config)#**event authentication-failure both**
event X-ring-topology-change [Systemlog|SMTP|Both]	G	Set X - ring topology changed event type	switch(config)#**event X-ring-topology-change both**
event systemlog [Link-UP|Link-Down|Both]	I	Set port event for system log	switch(config)#**interface fastethernet 3** switch(config-if)#**event systemlog both**
event smtp [Link-UP|Link-Down|Both]	I	Set port event for SMTP	switch(config)#**interface fastethernet 3** switch(config-if)#**event smtp both**
show event	P	Show event selection	switch#**show event**
no event device-cold-start	G	Disable cold start event type	switch(config)#**no event device-cold-start**
no event authentication-failure	G	Disable Authentication failure event type	switch(config)#**no event authentication-failure**
no event X-ring-topology-change	G	Disable X - ring topology changed event type	switch(config)#**no event X-ring-topology-change**
no event systemlog	I	Disable port event for system log	switch(config)#**interface fastethernet 3** switch(config-if)#**no event systemlog**
no event smpt	I	Disable port event for SMTP	switch(config)#**interface fastethernet 3** switch(config-if)#**no event smtp**
show systemlog	P	Show system log client & server information	switch#**show systemlog**

3.1.16 SNTP Commands Set

Table 3.16: SNTP Commands Set

Netstar Commands	Level	Description	Example
sntp enable	G	Enable SNTP function	switch(config)#**sntp enable**
sntp daylight	G	Enable daylight saving time, if SNTP function is inactive, this command can't be applied.	switch(config)#**sntp daylight**
sntp daylight-period [Start time] [End time]	G	Set period of daylight saving time, if SNTP function is inactive, this command can't be applied. Parameter format: [yyyymmdd-hh:mm]	switch(config)# **sntp daylight-period 20060101-01:01 20060202-01-01**
sntp daylight-offset [Minute]	G	Set offset of daylight saving time, if SNTP function is inactive, this command can't be applied.	switch(config)#**sntp daylight-offset 3**
sntp ip [IP]	G	Set SNTP server IP, if SNTP function is inactive, this command can't be applied.	switch(config)#**sntp ip 192.169.1.1**
sntp timezone [Timezone]	G	Set timezone index, use "show sntp timzezone" command to get more information of index number	switch(config)#**sntp timezone 22**
show sntp	P	Show SNTP information	switch#**show sntp**

show sntp timezone	**P**	Show index number of time zone list	switch#**show sntp timezone**
no sntp	**G**	Disable SNTP function	switch(config)#**no sntp**
no sntp daylight	**G**	Disable daylight saving time	switch(config)#**no sntp daylight**

3.1.17 X-ring Commands Set

Table 3.17: X-ring Commands Set

Netstar Commands	Level	Description	Example
Xring enable	**G**	Enable X-ring	switch(config)#**Xring enable**
Xring master	**G**	Enable ring master	switch(config)#**Xring master**
Xring couplering	**G**	Enable couple ring	switch(config)#**Xring couplering**
Xring dualhoming	**G**	Enable dual homing	switch(config)#**Xring dualhoming**
Xring ringport [1st Ring Port] [2nd Ring Port]	**G**	Configure 1st/2nd Ring Port	switch(config)#**Xring ringport 7 8**
Xring couplingport [Coupling Port]	**G**	Configure Coupling Port	switch(config)#**Xring couplingport 1**
Xring controlport [Control Port]	**G**	Configure Control Port	switch(config)#**Xring controlport 2**
Xring homingport [Dual Homing Port]	**G**	Configure Dual Homing Port	switch(config)#**Xring homingport 3**
show Xring	**P**	Show the information of X - Ring	switch#**show Xring**
no Xring	**G**	Disable X-ring	switch(config)#**no Xring**
no Xring master	**G**	Disable ring master	switch(config)# **no Xring master**
no Xring couplering	**G**	Disable couple ring	switch(config)# **no Xring couplering**
no Xring dualhoming	**G**	Disable dual homing	switch(config)# **no Xring dualhoming**

3.2 Web Browser

EKI-7758F provides a convenient configure way via web browser, you can follow below step to access EKI-7758F.

EKI-7758F's default IP is 192.168.1.1, make sure your host PC and EKI-7758F are on the same logical sub-network.

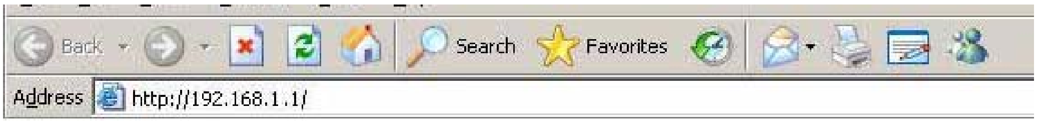
Warning *Your host PC should be in the same VLAN setting with EKI-7758F, or the management will not be configured.*

Connect EKI-7758F to the Ethernet then your host PC could configure it via Ethernet. Or you can directly connect EKI-7758F to your host PC with a straight-through or cross over Ethernet cable.

Before to use web management, install the industrial switch on the network and make sure that any one of PC on the network can connect with the industrial switch through the web browser. The industrial switch default value of IP, subnet mask, username and password is as below:

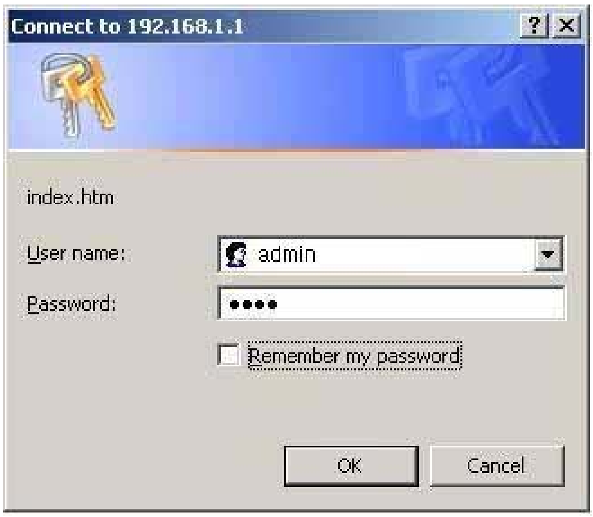
- IP Address: 192.168.1.1
- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.1.254
- User Name: admin
- Password: admin

Open Internet Explorer and type EKI-7758F's IP in the Address field then press Enter to open the web login page.



Address http://192.168.1.1/

Figure 3.5: Type the address in the URL


Connect to 192.168.1.1

index.htm

User name: admin

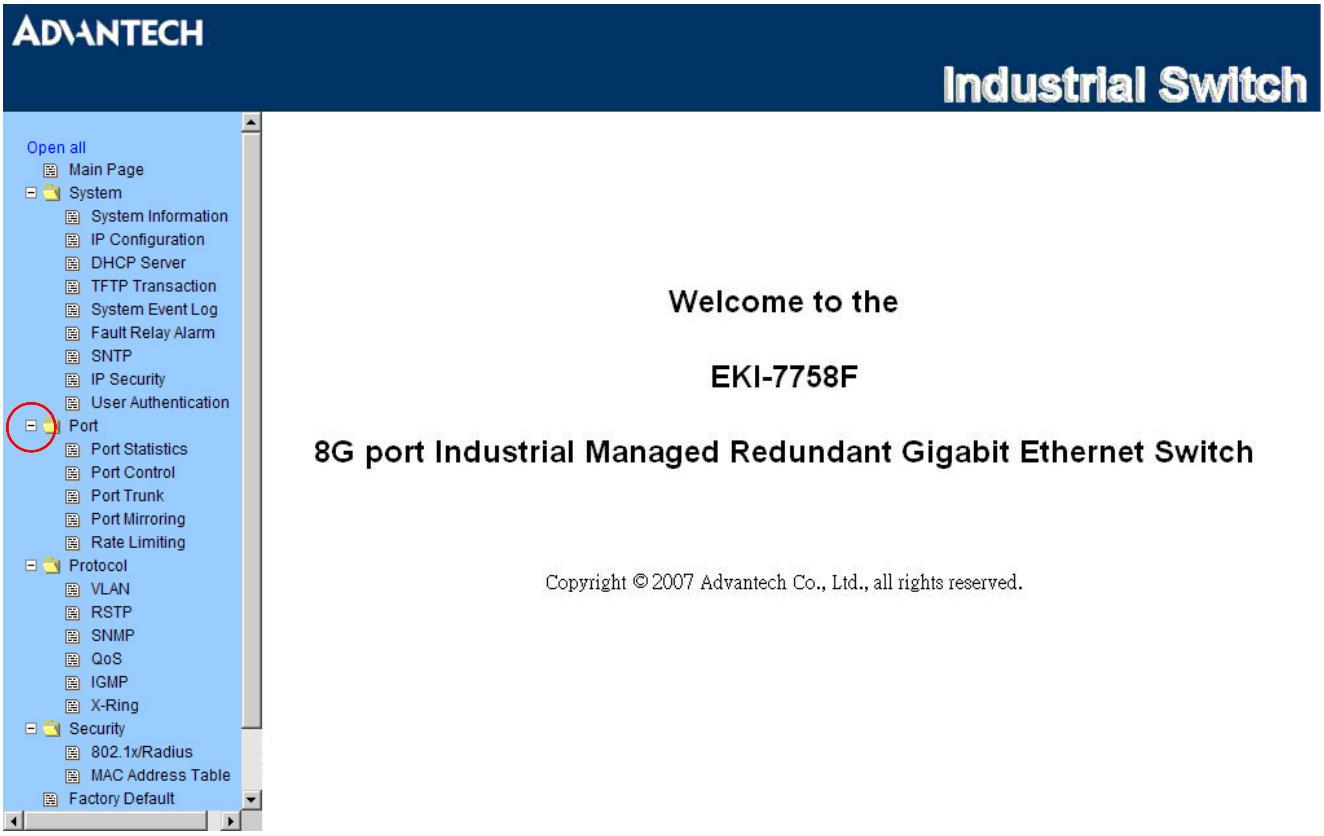
Password: ●●●●

□ Remember my password

Figure 3.6: Web Login Window

Default user name and password are both **admin**, fill in the user name and password then press **OK** to enter the configuration. You can change the password in the system setting.

In the main page, you can find the tree menu structure of the EKI-7758F in the left side. Click the "+" symbol to unroll the hiding hyperlink, and click the hyperlink to open the function page you want to configure.



Welcome to the

EKI-7758F

8G port Industrial Managed Redundant Gigabit Ethernet Switch

Copyright © 2007 Advantech Co., Ltd., all rights reserved.

Figure 3.7: Main page

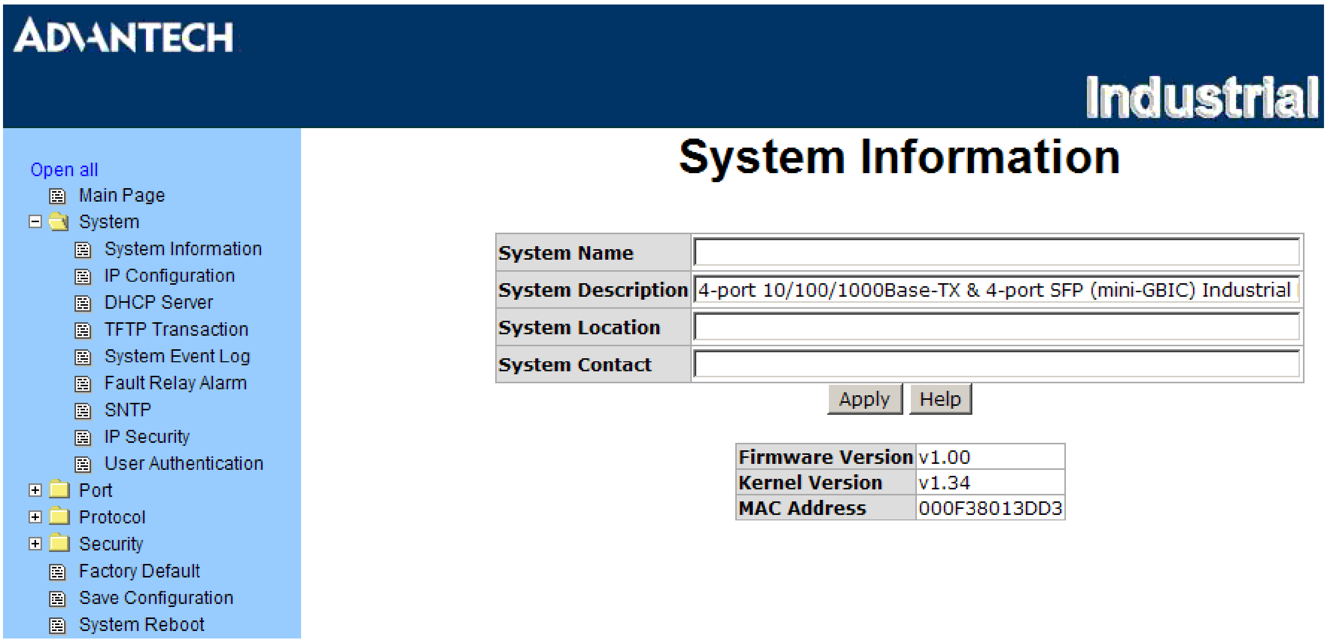
3.2.1 System

System Information

Assign the system name, location and view the system information

- **System Name**: Assign the name of the switch. The maximum length is 64 bytes.
- **System Description**: Displays the description of switch. Read only cannot be modified.
- **System Location**: Assign the switch physical location. The maximum length is 64 bytes.
- **System Contact**: Enter the name of contact person or organization.
- **Firmware Version**: Displays the switch's firmware version.
- **Kernel Version**: Displays the kernel software version.
- **MAC Address**: Displays the unique hardware address assigned by manufacturer (default).

Warning *Don't set "0" for the first segment of the subnet mask and default gateway (000.xxx.xxx.xxx).*
Refresh the web screen if the web could not be displayed while you change the setting.



System Information

System Name	
System Description	4-port 10/100/1000Base-TX & 4-port SFP (mini-GBIC) Industrial
System Location	
System Contact	

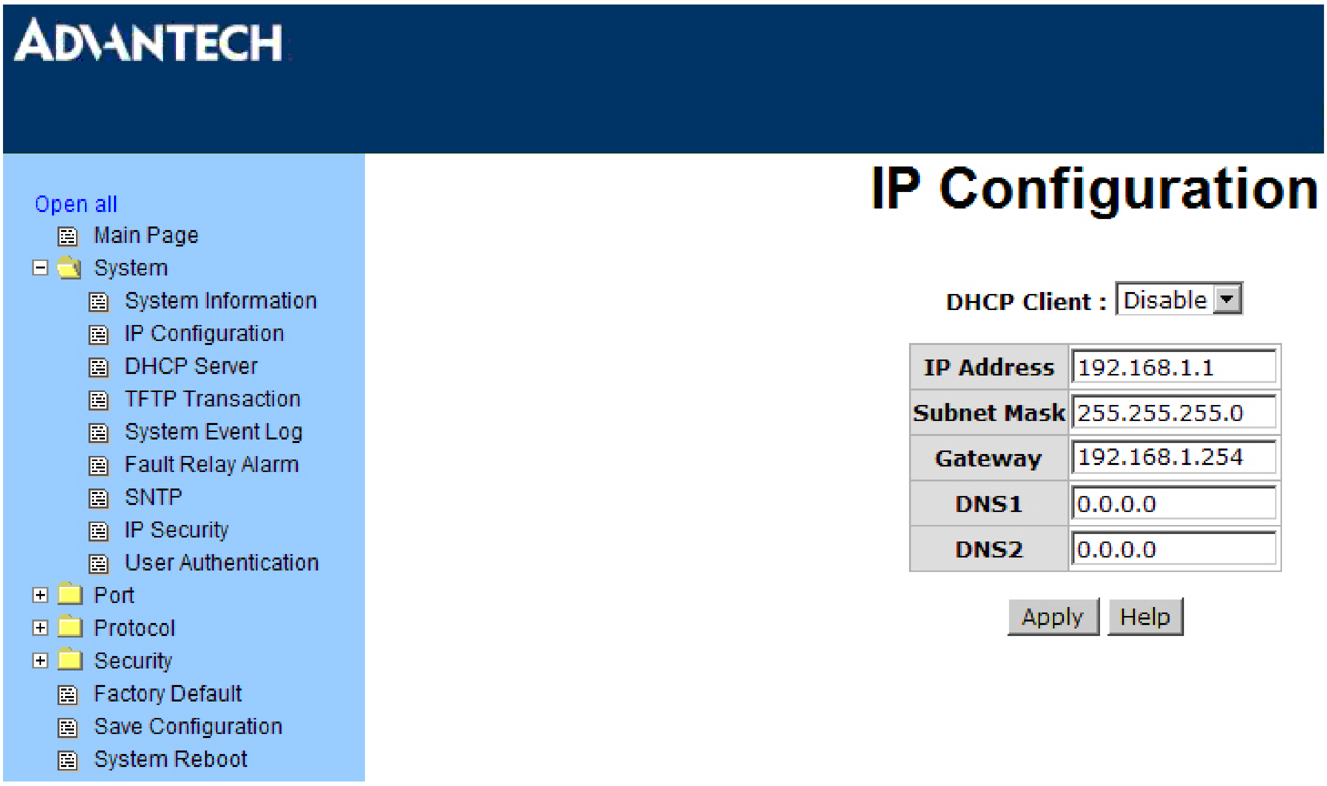
Firmware Version	v1.00
Kernel Version	v1.34
MAC Address	000F38013DD3

Figure 3.8: System Information

IP Configuration

User can configure the IP Settings and DHCP client function here.

- **DHCP Client**: To enable or disable the DHCP client function. When DHCP client function is enabling, the industrial switch will be assigned the IP address from the network DHCP server. The default IP address will be replace by the DHCP server assigned IP address. After user click “Apply” button, a popup dialog show up. It is to inform the user that when the DHCP client is enabling, the current IP will lose and user should find the new IP on the DHCP server.
- **IP Address**: Assign the IP address that the network is using. If DHCP client function is enabling, and then user doesn’t need to assign the IP address. And, the network DHCP server will assign the IP address for the industrial switch and displays in this column. The default IP is 192.168.1.1.
- **Subnet Mask**: Assign the subnet mask of the IP address. If DHCP client function is enabling, and then user does not need to assign the subnet mask.
- **Gateway**: Assign the network gateway for the industrial switch. The default gateway is 192.168.1.254.
- **DNS1**: Assign the primary DNS IP address.
- **DNS2**: Assign the secondary DNS IP address.
- And then, click Apply



IP Configuration

DHCP Client : Disable

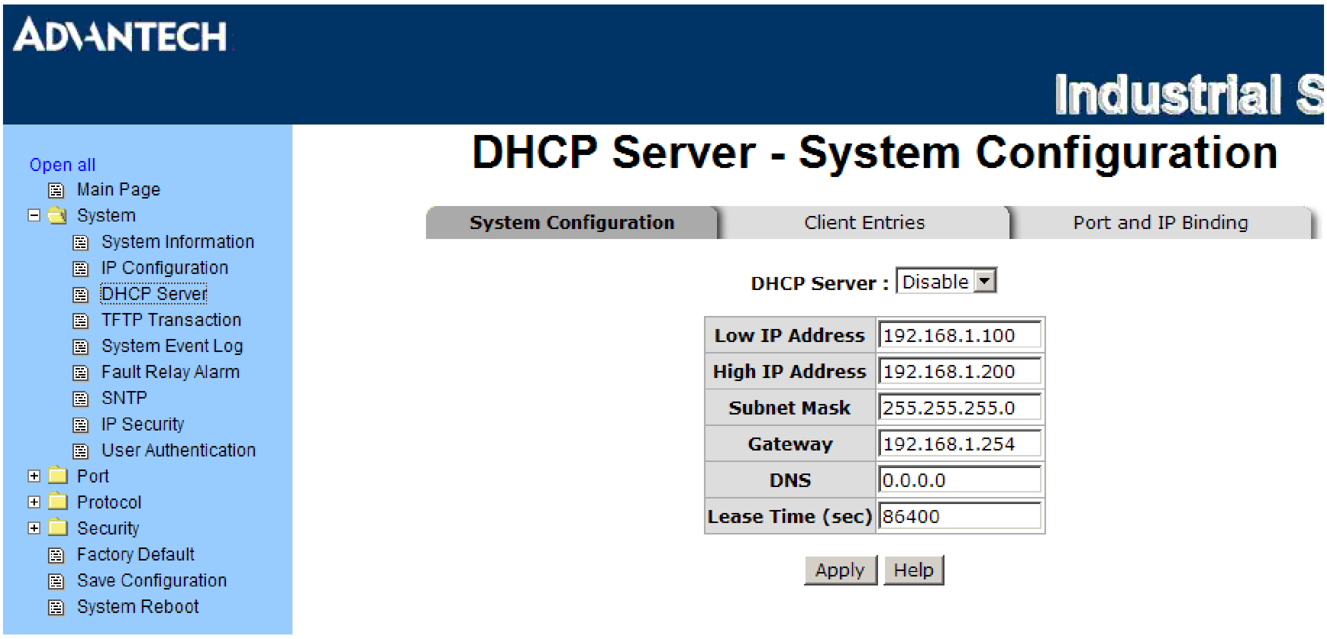
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Gateway	192.168.1.254
DNS1	0.0.0.0
DNS2	0.0.0.0

Figure 3.9: IP Configuration

DHCP Server – System configuration

The system provides the DHCP server function. Enable the DHCP server function, the switch system will be a DHCP server.

- **DHCP Server:** Enable or Disable the DHCP Server function. Enable – the switch will be the DHCP server on your local network.
- **Low IP Address:** the dynamic IP assign range. Low IP address is the beginning of the dynamic IP assigns range. For example: dynamic IP assign range is from 192.168.1.100 ~ 192.168.1.200. 192.168.1.100 will be the Low IP address.
- **High IP Address:** the dynamic IP assign range. High IP address is the end of the dynamic IP assigns range. For example: dynamic IP assign range is from 192.168.1.100 ~ 192.168.1.200. 192.168.1.200 will be the High IP address.
- **Subnet Mask:** the dynamic IP assign range subnet mask.
- **Gateway:** the gateway in your network.
- **DNS:** Domain Name Server IP Address in your network.
- **Lease Time (sec):** It is the time period that system will reset the dynamic IP assignment to ensure the dynamic IP will not been occupied for a long time or the server doesn't know that the dynamic IP is idle.
- And then, click Apply



DHCP Server - System Configuration

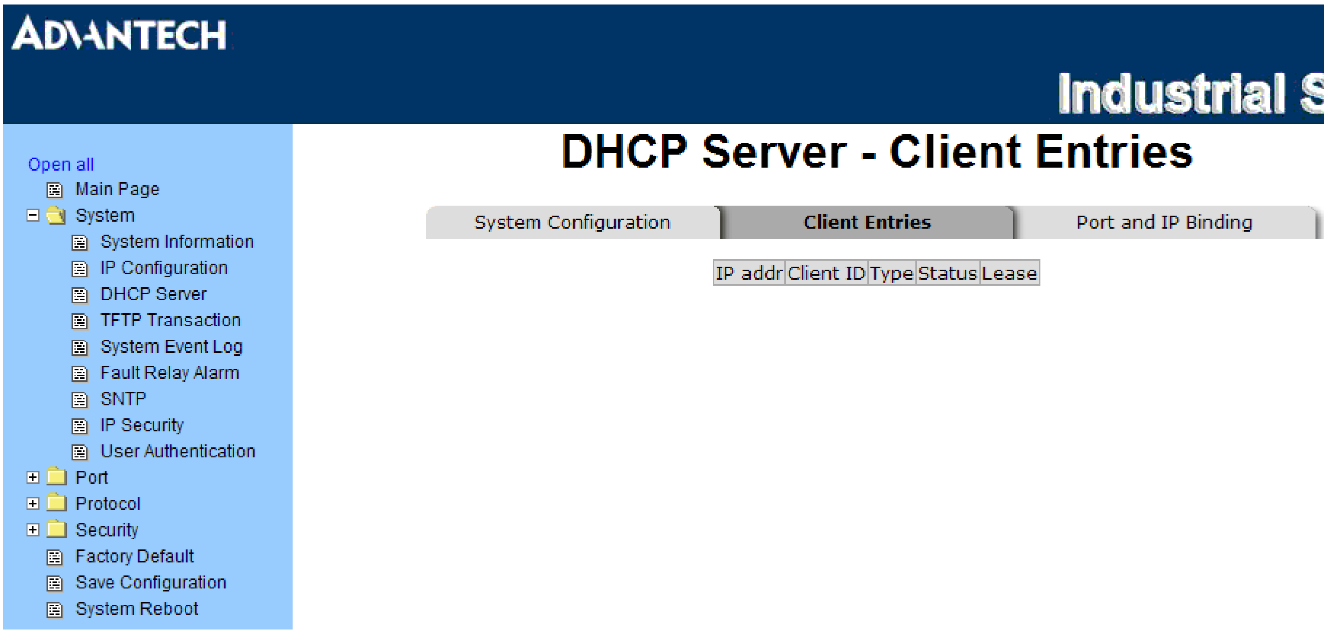
DHCP Server : Disable

Low IP Address	192.168.1.100
High IP Address	192.168.1.200
Subnet Mask	255.255.255.0
Gateway	192.168.1.254
DNS	0.0.0.0
Lease Time (sec)	86400

Figure 3.10: DHCP Server - System Configuration

DHCP Client – System Configuration

When the DHCP server function is active, the system will collect the DHCP client information and displays it here.



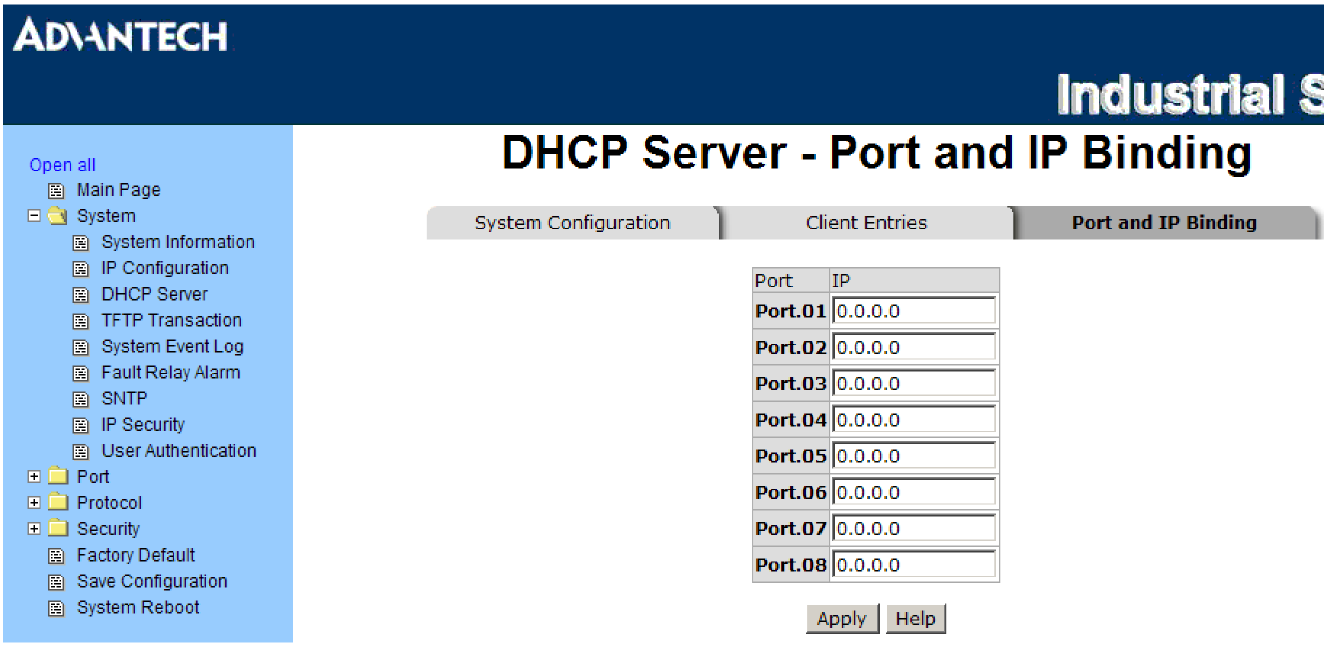
DHCP Server - Client Entries

IP addr	Client ID	Type	Status	Lease

Figure 3.11: DHCP Server – Client Entries

DHCP Server - Port and IP Bindings

You can assign the specific IP address that is the IP in dynamic IP assign range to the specific port. When the device is connecting to the port and asks for dynamic IP assigning, the system will assign the IP address that has been assigned before to the connected device.



DHCP Server - Port and IP Binding

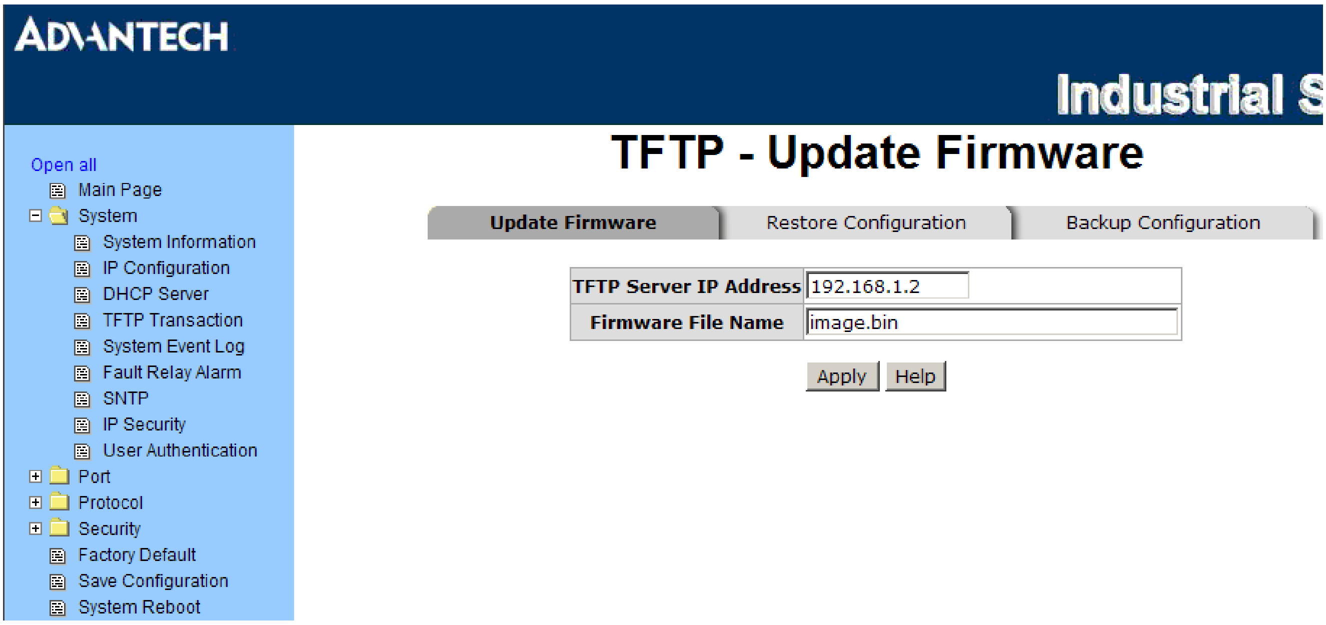
Port	IP
Port.01	0.0.0.0
Port.02	0.0.0.0
Port.03	0.0.0.0
Port.04	0.0.0.0
Port.05	0.0.0.0
Port.06	0.0.0.0
Port.07	0.0.0.0
Port.08	0.0.0.0

Figure 3.12: DHCP Server – Client Entries

TFTP - Update Firmware

It provides the functions to allow a user to update the switch firmware. Before updating, make sure you have your TFTP server ready and the firmware image is on the TFTP server.

- **TFTP Server IP Address:** fill in your TFTP server IP.
- **Firmware File Name:** the name of firmware image.
- And then, click Apply



TFTP - Update Firmware

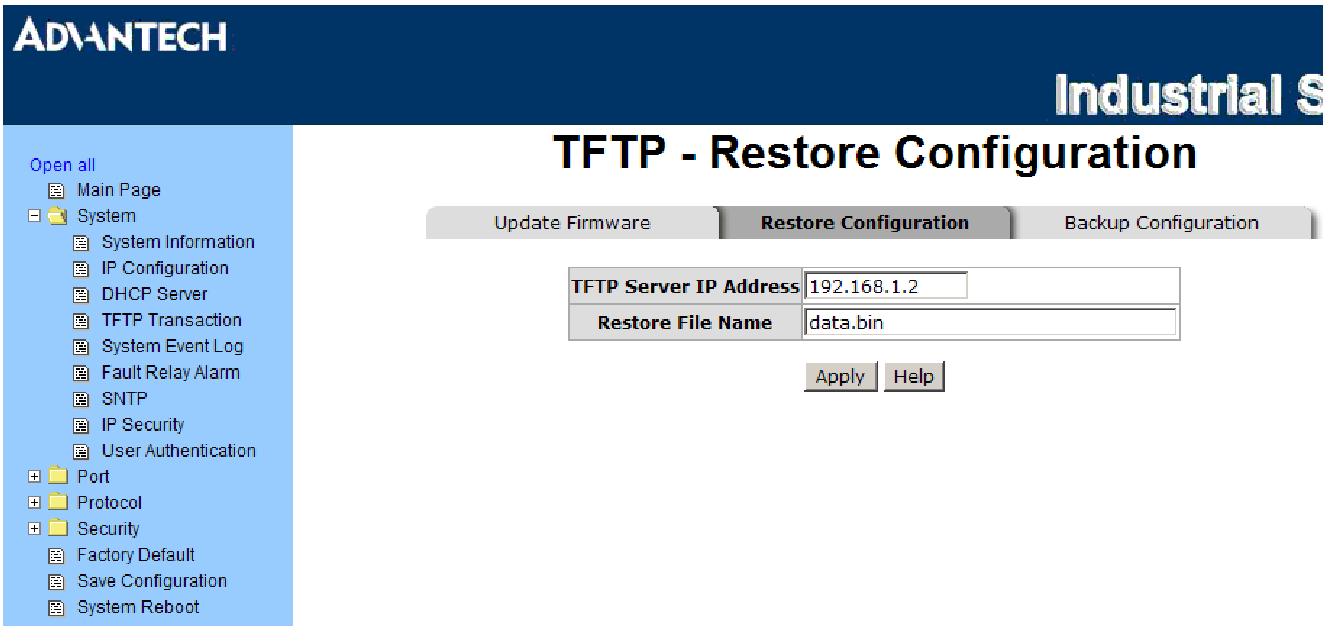
TFTP Server IP Address	192.168.1.2
Firmware File Name	image.bin

Figure 3.13: TFTP – Update Firmware

TFTP – Restore Configuration

You can restore Flash ROM value from TFTP server, but you must put the image file on TFTP server first, switch will download back flash image.

- **TFTP Server IP Address:** fill in the TFTP server IP.
- **Restore File Name:** fill in the correct restore file name.
- Click Apply



TFTP - Restore Configuration

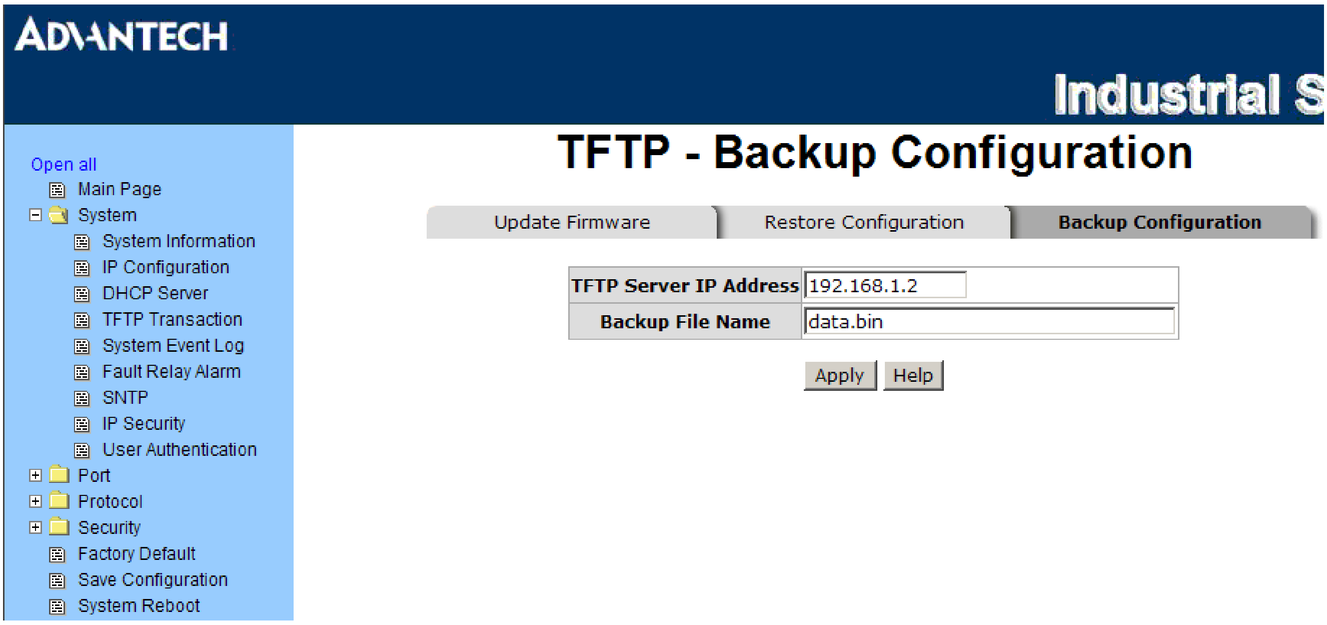
TFTP Server IP Address	192.168.1.2
Restore File Name	data.bin

Figure 3.14: TFTP – Restore Configuration

TFTP - Backup Configuration

You can save current Flash ROM value from the switch to TFTP server, then go to the TFTP restore configuration page to restore the Flash ROM value.

- **TFTP Server IP Address:** fill in the TFTP server IP
- **Backup File Name:** fill the file name
- Click Apply.



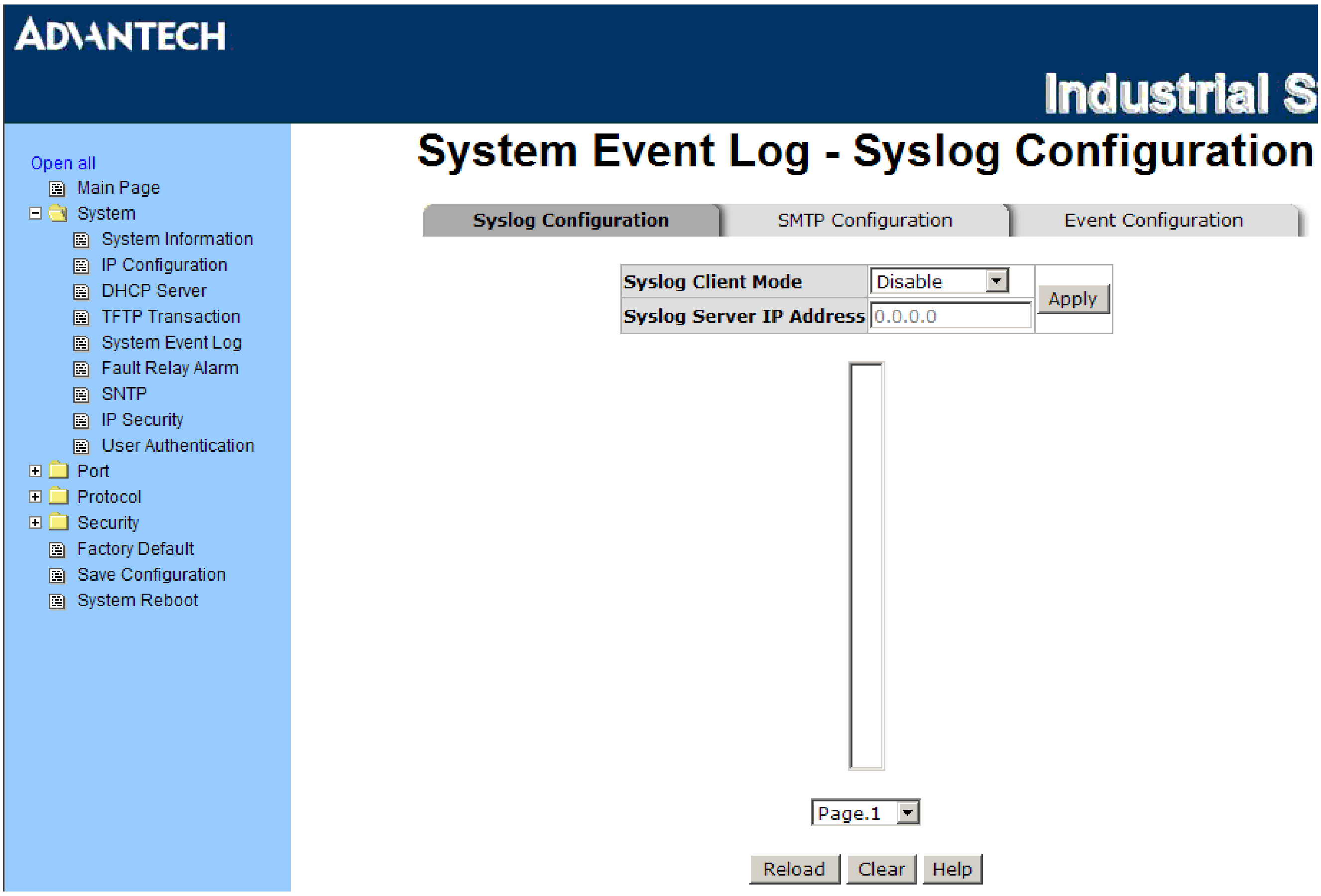
TFTP Server IP Address	192.168.1.2
Backup File Name	data.bin

Figure 3.15: TFTP – Backup Configuration

System Event Log – Syslog Configuration

Configuring the system event mode that want to be collected and system log server IP.

- **Syslog Client Mode:** select the system log mode – client only, server only, or both S/C.
- **System Log Server IP Address:** assigned the system log server IP.
- Click Reload to refresh the events log.
- Click Clear to clear all current events log.
- After configuring, Click Apply.



System Event Log - Syslog Configuration

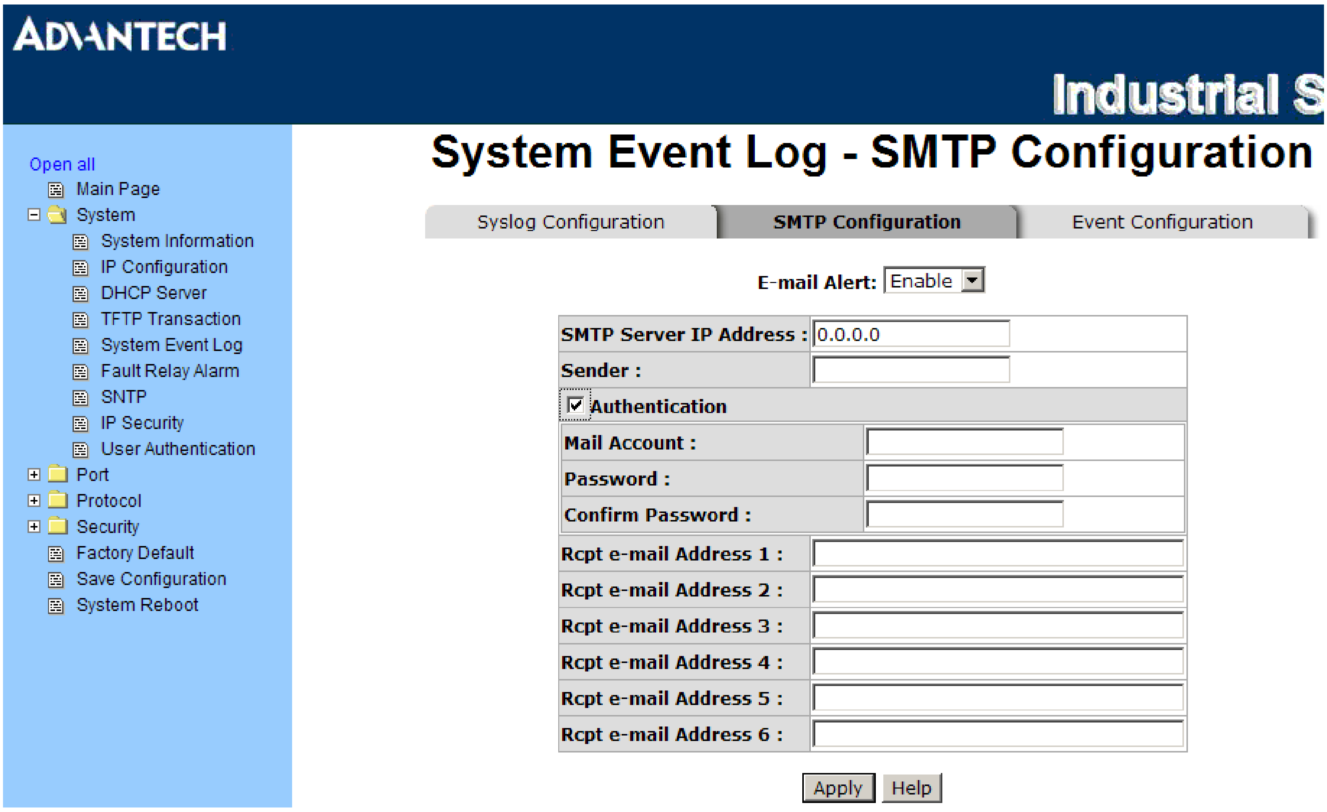
Syslog Client Mode	Disable
Syslog Server IP Address	0.0.0.0

Figure 3.16: Syslog Configuration

System Event Log - SMTP Configuration

You can set up the mail server IP, mail account, account password, and forwarded email account for receiving the event alert.

- **Email Alert:** enable or disable the email alert function.
- **SMTP Server IP:** set up the mail server IP address (when Email Alert enabled, this function will then be available).
- **Authentication:** mark the check box to enable and configure the email account and password for authentication (when Email Alert enabled, this function will then be available).
- **Mail Account:** set up the email account, e.g. johnadmin@123.com, to receive the alert. It must be an existing email account on the mail server, which you had set up in SMTP Server IP Address column.
- **Password:** The email account password.
- **Confirm Password:** reconfirm the password.
- **Rcpt e-mail Address 1 ~ 6:** you can assign up to 6 e-mail accounts also to receive the alert.
- Click Apply.



System Event Log - SMTP Configuration

E-mail Alert: Enable

SMTP Server IP Address :	0.0.0.0
Sender :	
☑ Authentication	
Mail Account :	
Password :	
Confirm Password :	
Rcpt e-mail Address 1 :	
Rcpt e-mail Address 2 :	
Rcpt e-mail Address 3 :	
Rcpt e-mail Address 4 :	
Rcpt e-mail Address 5 :	
Rcpt e-mail Address 6 :	

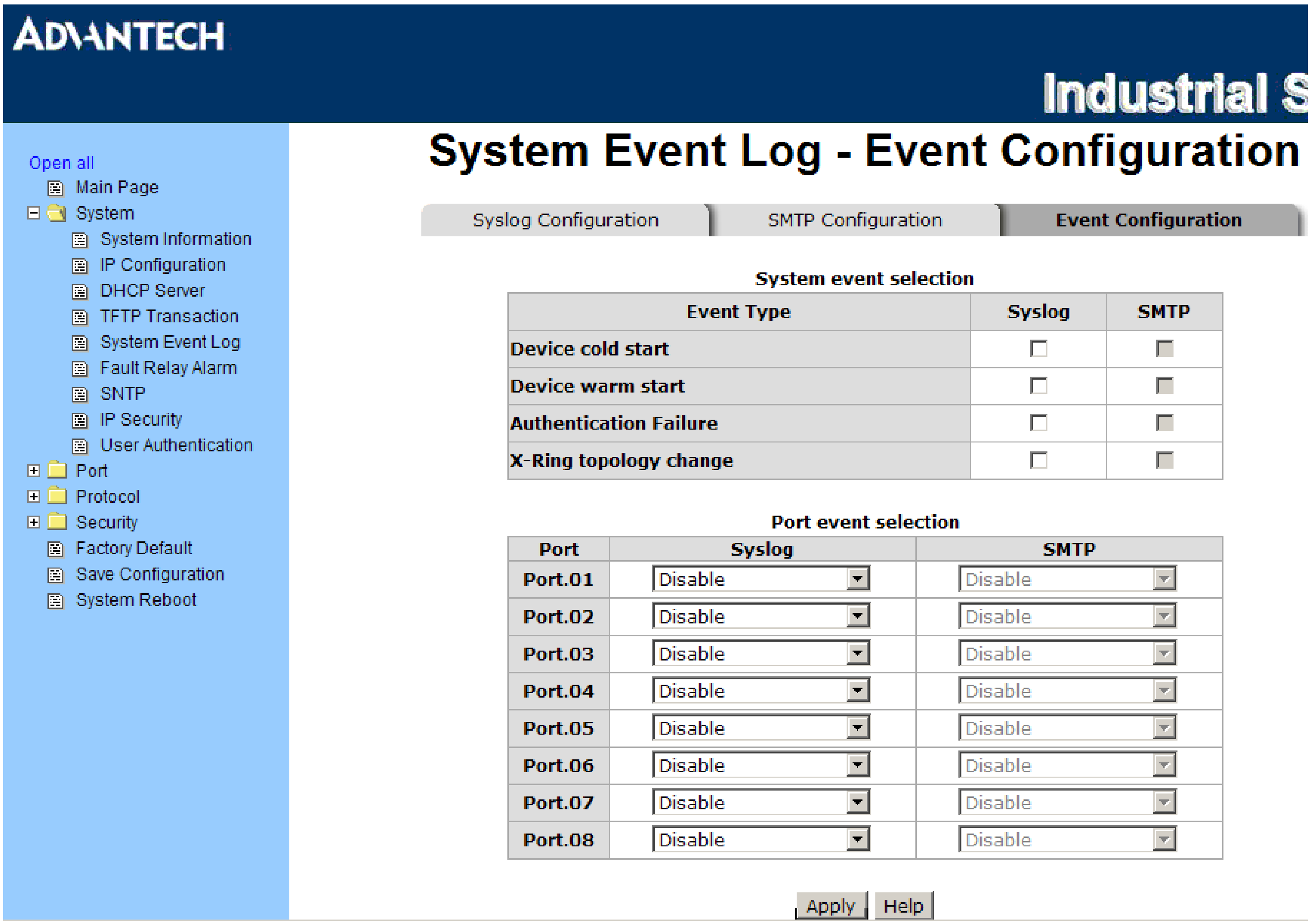
Figure 3.17: SMTP Configuration

System Event Log - Event Configuration

You can select the system log events and SMTP events. When selected events occur, the system will send out the log information. Also, per port log and SMTP events can be selected. After configure, Click Apply.

- **System event selection:** 4 selections – Device cold start, Device warm start, SNMP Authentication Failure, and X-ring topology change. Mark the checkbox to select the event. When selected events occur, the system will issue the logs.
  - **Device cold start:** when the device executes cold start action, the system will issue a log event.
  - **Device warm start:** when the device executes warm start, the system will issue a log event.
  - **Authentication Failure:** when the SNMP authentication fails, the system will issue a log event.
  - **X-ring topology change:** when the X-ring topology has changed, the system will issue a log event.

- **Port event selection:** select the per port events and per port SMTP events. It has 3 selections – **Link Up**, **Link Down**, and **Link UP & Link Down**. Disable means no event is selected.
  - **Link UP:** the system will issue a log message when port connection is up only.
  - **Link Down:** the system will issue a log message when port connection is down only.
  - **Link UP & Link Down:** the system will issue a log message when port connection is up and down.



System Event Log - Event Configuration

System event selection

Event Type	Syslog	SMTP
Device cold start	□	□
Device warm start	□	□
Authentication Failure	□	□
X-Ring topology change	□	□

Port event selection

Port	Syslog	SMTP
Port.01	Disable	Disable
Port.02	Disable	Disable
Port.03	Disable	Disable
Port.04	Disable	Disable
Port.05	Disable	Disable
Port.06	Disable	Disable
Port.07	Disable	Disable
Port.08	Disable	Disable

Figure 3.18: Event Configuration

Fault Relay Alarm

- **Power Failure:** Mark the check box to enable the function of lighting up FAULT LED on the panel when power fails.
- **Port Link Down/Broken:** Mark the check box to enable the function of lighting up FAULT LED on the panel when Ports' states are link down or broken.

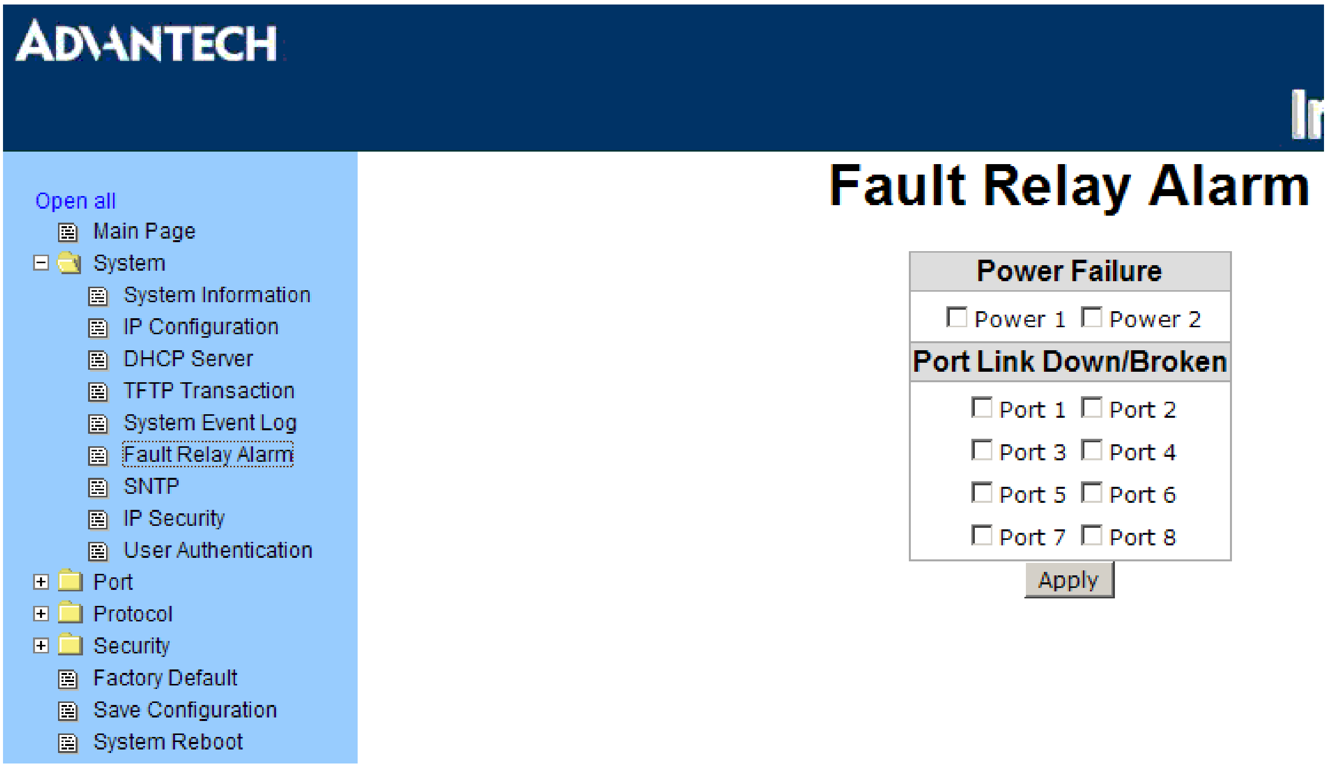


Figure 3.19: Fault Relay Alarm

SNTP Configuration

You can configure the SNTP (Simple Network Time Protocol) settings. The SNTP allows you to synchronize switch clocks in the Internet.

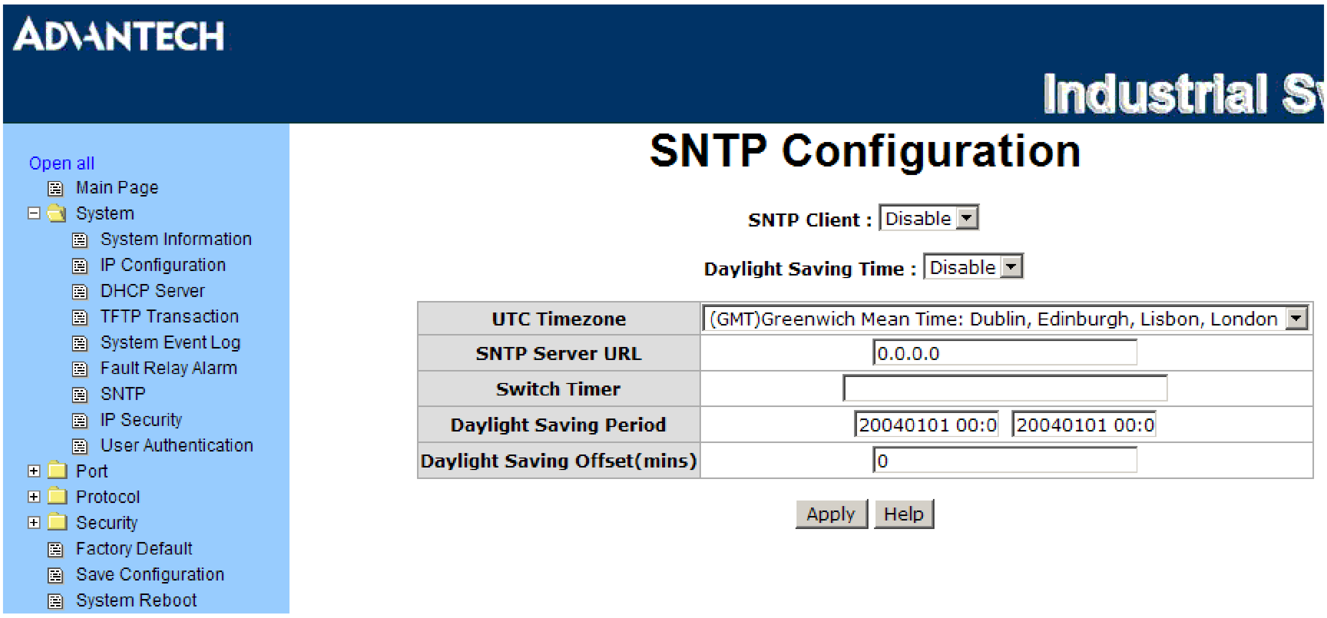
- **SNTP Client:** enable or disable SNTP function to get the time from the SNTP server.
- **Daylight Saving Time:** enable or disable daylight saving time function. When daylight saving time is enabled, you need to configure the daylight saving time period.
- **UTC Timezone:** set the switch location time zone. The following table lists the different location time zone for your reference.

Table 3.18: UTC Timezone

Local Time Zone	Conversion from UTC	Time at 12:00 UTC
November Time Zone	- 1 hour	11am
Oscar Time Zone	-2 hours	10 am
ADT - Atlantic Daylight	-3 hours	9 am
AST - Atlantic Standard EDT - Eastern Daylight	-4 hours	8 am
EST - Eastern Standard CDT - Central Daylight	-5 hours	7 am

CST - Central Standard MDT - Mountain Daylight	-6 hours	6 am
MST - Mountain Standard PDT - Pacific Daylight	-7 hours	5 am
PST - Pacific Standard ADT - Alaskan Daylight	-8 hours	4 am
ALA - Alaskan Standard	-9 hours	3 am
HAW - Hawaiian Standard	-10 hours	2 am
Nome, Alaska	-11 hours	1 am
CET - Central European FWT - French Winter MET - Middle European MEWT - Middle European Winter SWT - Swedish Winter	+1 hour	1 pm
EET - Eastern European, USSR Zone 1	+2 hours	2 pm
BT - Baghdad, USSR Zone 2	+3 hours	3 pm
ZP4 - USSR Zone 3	+4 hours	4 pm
ZP5 - USSR Zone 4	+5 hours	5 pm
ZP6 - USSR Zone 5	+6 hours	6 pm
WAST - West Australian Standard	+7 hours	7 pm
CCT - China Coast, USSR Zone 7	+8 hours	8 pm
JST - Japan Standard, USSR Zone 8	+9 hours	9 pm
EAST - East Australian Standard GST Guam Standard, USSR Zone 9	+10 hours	10 pm
IDLE - International Date Line NZST - New Zealand Standard NZT - New Zealand	+12 hours	Midnight

- **SNTP Sever URL:** set the SNTP server IP address.
- **Daylight Saving Period:** set up the Daylight Saving beginning time and Daylight Saving ending time. Both will be different in every year.
- **Daylight Saving Offset (mins):** set up the offset time.
- **Switch Timer:** Displays the switch current time.
- Click Apply .



SNTP Configuration

SNTP Client : Disable

Daylight Saving Time : Disable

UTC Timezone	(GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London
SNTP Server URL	0.0.0.0
Switch Timer	
Daylight Saving Period	20040101 00:0 20040101 00:0
Daylight Saving Offset(mins)	0

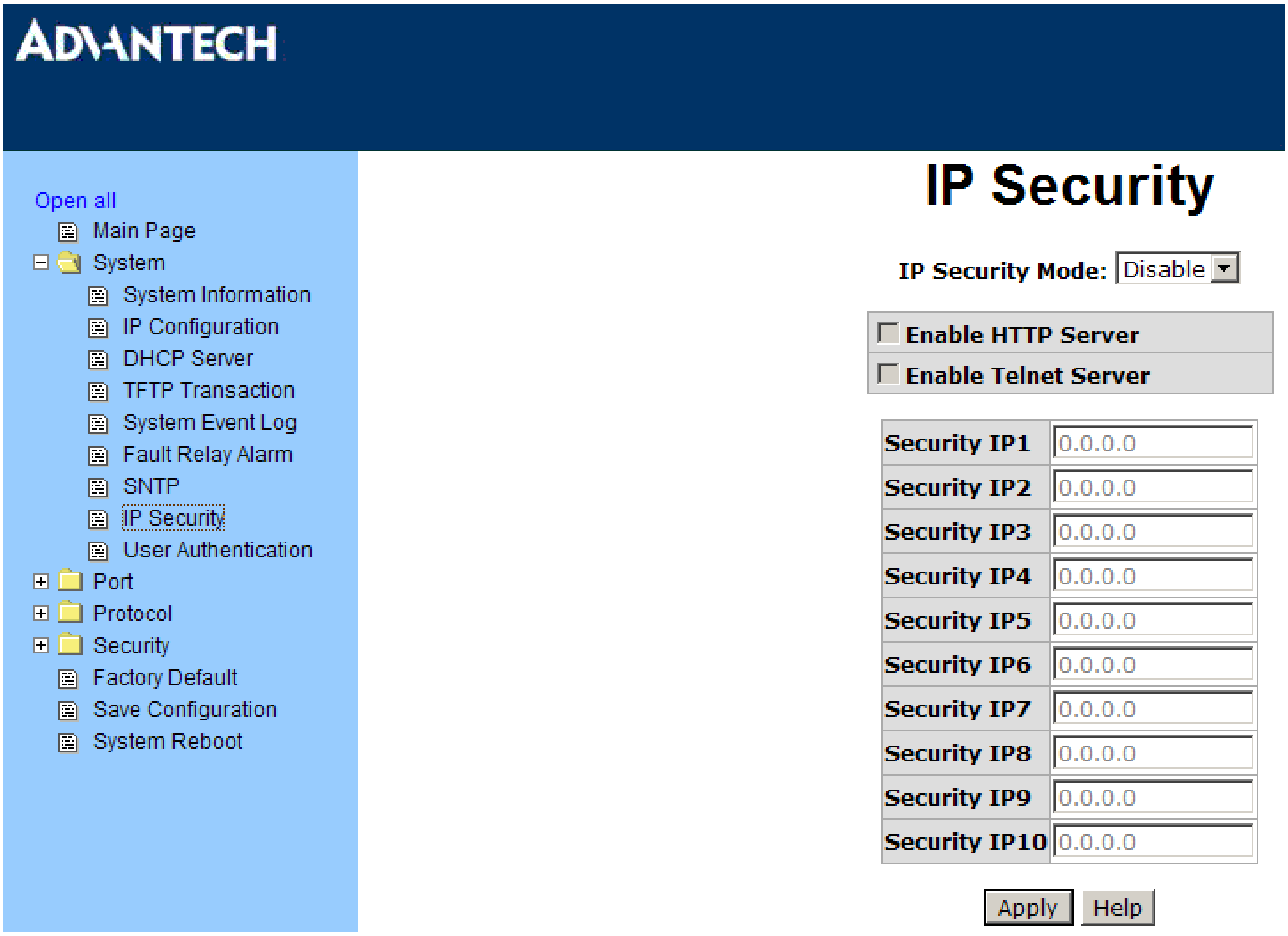
Figure 3.20: SNTP Configuration

IP Security

IP security function allows user to assign 10 specific IP addresses that have permission to access the switch through the web browser for the securing switch management.

- **IP Security Mode:** when this option is in Enable mode, the Enable HTTP Server and Enable Telnet Server check boxes will then be available.
- **Enable HTTP Server:** when this check box is checked, the IP addresses among Security IP1 ~ IP10 will be allowed to access via HTTP service.
- **Enable Telnet Server:** when checked, the IP addresses among Security IP1 ~ IP10 will be allowed to access via telnet service.
- **Security IP 1 ~ 10:** Assign up to 10 specific IP address. Only these 10 IP address can access and manage the switch through the Web browser
- And then, click Apply button to apply the configuration.

Note *Remember to execute the "Save Configuration" action, otherwise the new configuration will lose when switch power off.*



IP Security

IP Security Mode: Disable

□ Enable HTTP Server

□ Enable Telnet Server

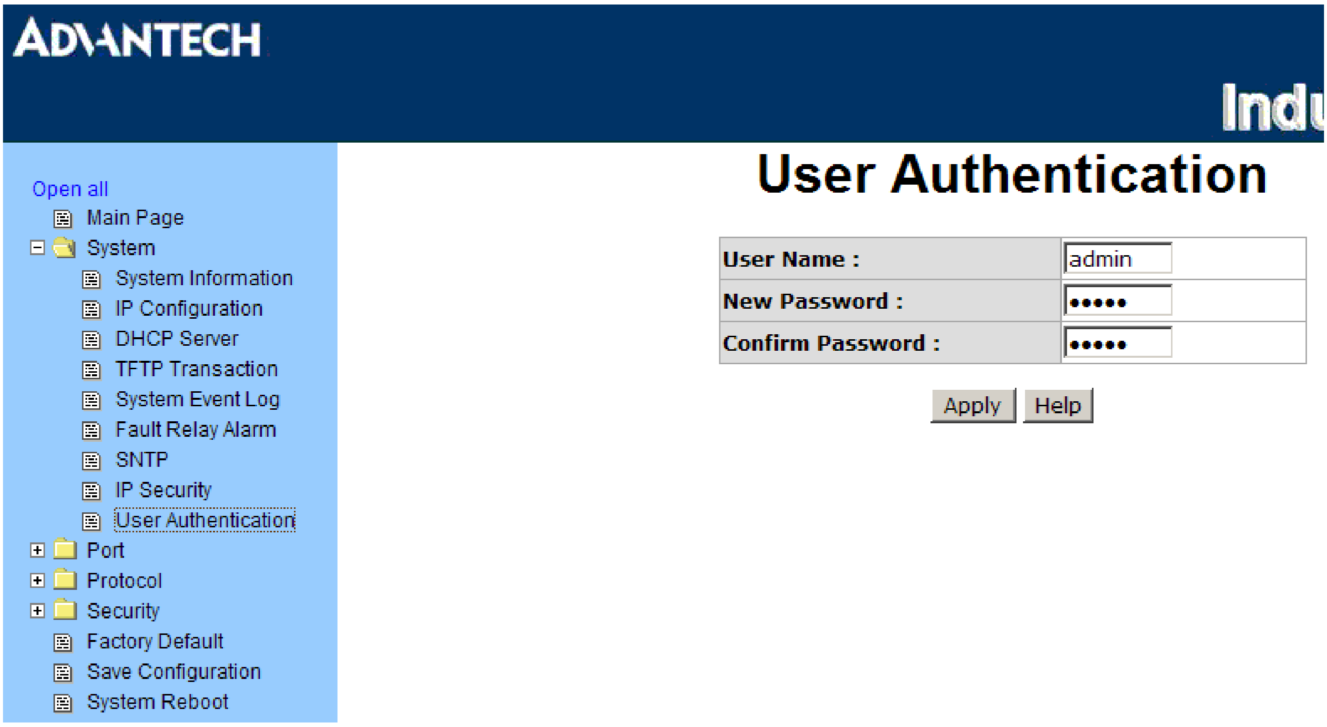
Security IP1	0.0.0.0
Security IP2	0.0.0.0
Security IP3	0.0.0.0
Security IP4	0.0.0.0
Security IP5	0.0.0.0
Security IP6	0.0.0.0
Security IP7	0.0.0.0
Security IP8	0.0.0.0
Security IP9	0.0.0.0
Security IP10	0.0.0.0

Figure 3.21: IP Security

User Authentication

Change web management login user name and password for the management security issue.

- **User name:** Key in the new user name (The default is “admin”)
- **Password:** Key in the new password (The default is “admin”)
- **Confirm password:** Re-type the new password
- And then, click Apply button to apply the configuration.



User Authentication

User Name :	admin
New Password :	•••••
Confirm Password :	•••••

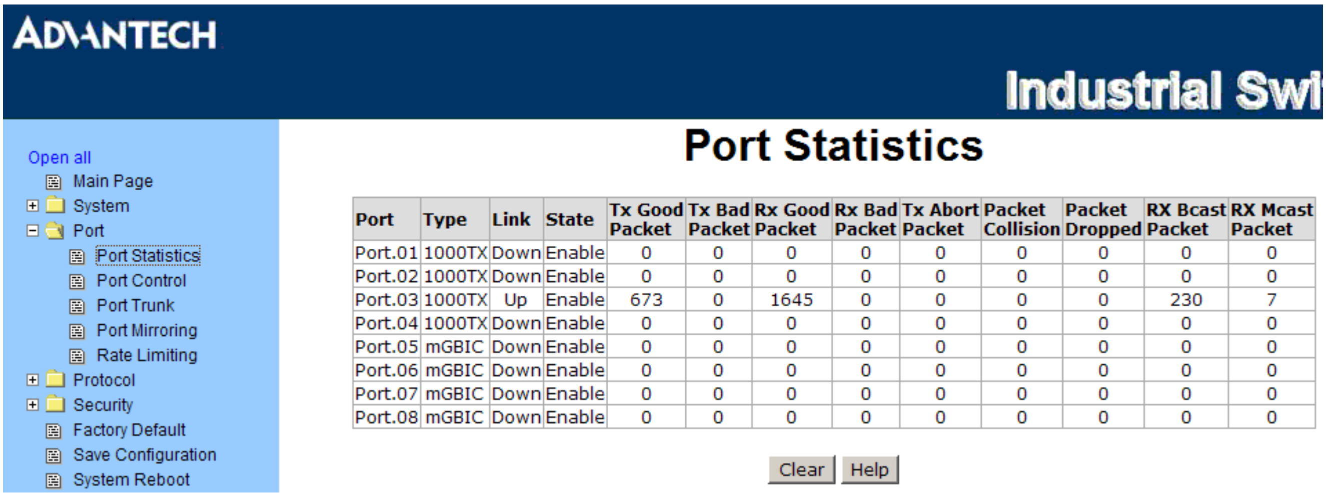
Figure 3.22: User Authentication

3.2.2 Port

Port Statistics

The following information provides the current port statistic information.

- **Port:** The port number.
- **Type:** Displays the current speed of connection to the port.
- **Link:** The status of linking—‘Up’ or ‘Down’.
- **State:** It’s set by Port Control. When the state is disabled, the port will not transmit or receive any packet.
- **Tx Good Packet:** The counts of transmitting good packets via this port.
- **Tx Bad Packet:** The counts of transmitting bad packets (including undersize [less than 64 octets], oversize, CRC Align errors, fragments and jabbers packets) via this port.
- **Rx Good Packet:** The counts of receiving good packets via this port.
- **Rx Bad Packet:** The counts of receiving good packets (including undersize [less than 64 octets], oversize, CRC error, fragments and jabbers) via this port.
- **Tx Abort Packet:** The aborted packet while transmitting.
- **Packet Collision:** The counts of collision packet.
- **Packet Dropped:** The counts of dropped packet.
- **Rx Bcast Packet:** The counts of broadcast packet.
- **Rx Mcast Packet:** The counts of multicast packet.
- click Apply button to apply the configuration.



Port Statistics

Port	Type	Link	State	Tx Good Packet	Tx Bad Packet	Rx Good Packet	Rx Bad Packet	Tx Abort Packet	Packet Collision	Packet Dropped	RX Bcast Packet	RX Mcast Packet
Port.01	1000TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.02	1000TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.03	1000TX	Up	Enable	673	0	1645	0	0	0	0	230	7
Port.04	1000TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.05	mGBIC	Down	Enable	0	0	0	0	0	0	0	0	0
Port.06	mGBIC	Down	Enable	0	0	0	0	0	0	0	0	0
Port.07	mGBIC	Down	Enable	0	0	0	0	0	0	0	0	0
Port.08	mGBIC	Down	Enable	0	0	0	0	0	0	0	0	0

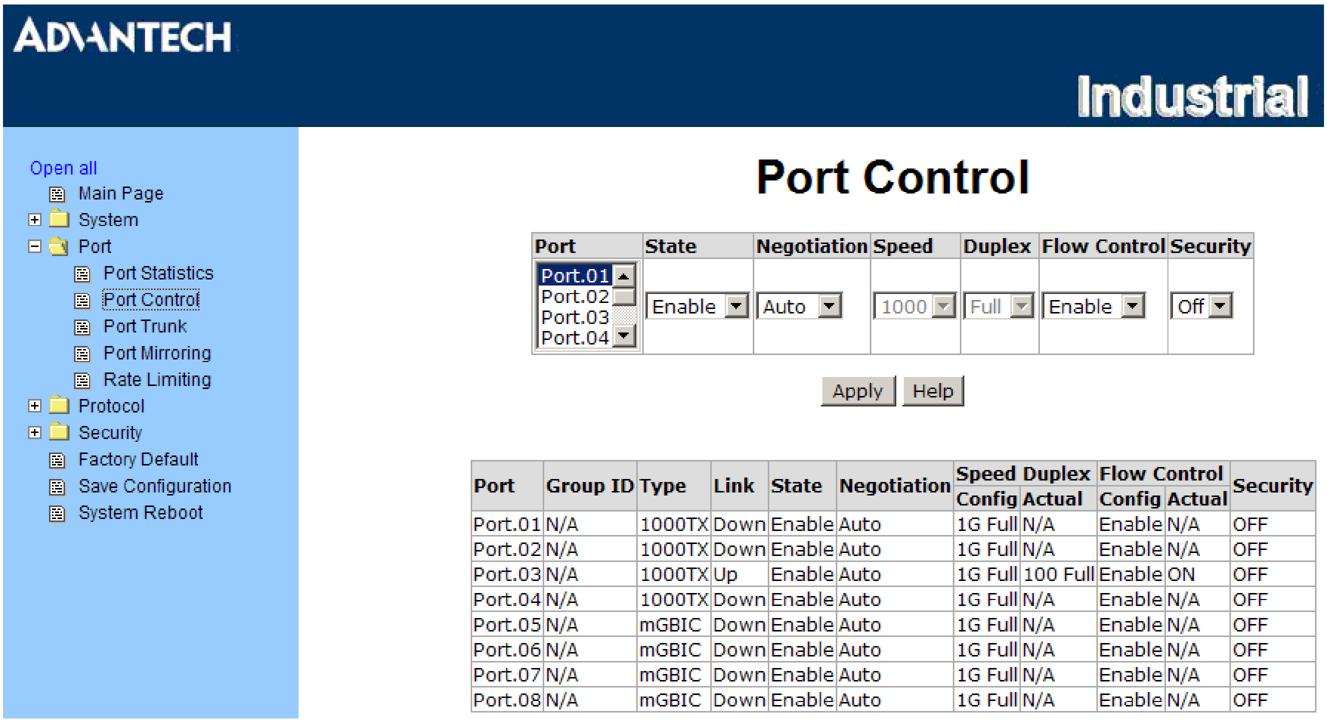
Figure 3.23: Port Statistics

Port Control

In Port control, you can view every port status that depended on user setting and the negotiation result.

- **Port:** select the port that you want to configure.
- **State:** current port status. The port can be set to disable or enable mode. If the port setting is disable then will not receive or transmit any packet.
- **Negotiation:** set auto negotiation status of port.
- **Speed:** set the port link speed.
- **Duplex:** set full-duplex or half-duplex mode of the port.
- **Flow Control:** set flow control function is Symmetric or Asymmetric in Full Duplex mode. The default value is Symmetric.
- **Security:** when its state is “On” that means this port accepts only one MAC address.

- Click Apply button to apply the configuration.



Port Control

Port	State	Negotiation	Speed	Duplex	Flow Control	Security
Port.01 Port.02 Port.03 Port.04	Enable	Auto	1000	Full	Enable	Off

Port	Group ID	Type	Link	State	Negotiation	Speed Duplex		Flow Control		Security
						Config	Actual	Config	Actual	
Port.01	N/A	1000TX	Down	Enable	Auto	1G Full	N/A	Enable	N/A	OFF
Port.02	N/A	1000TX	Down	Enable	Auto	1G Full	N/A	Enable	N/A	OFF
Port.03	N/A	1000TX	Up	Enable	Auto	1G Full	100 Full	Enable	ON	OFF
Port.04	N/A	1000TX	Down	Enable	Auto	1G Full	N/A	Enable	N/A	OFF
Port.05	N/A	mGBIC	Down	Enable	Auto	1G Full	N/A	Enable	N/A	OFF
Port.06	N/A	mGBIC	Down	Enable	Auto	1G Full	N/A	Enable	N/A	OFF
Port.07	N/A	mGBIC	Down	Enable	Auto	1G Full	N/A	Enable	N/A	OFF
Port.08	N/A	mGBIC	Down	Enable	Auto	1G Full	N/A	Enable	N/A	OFF

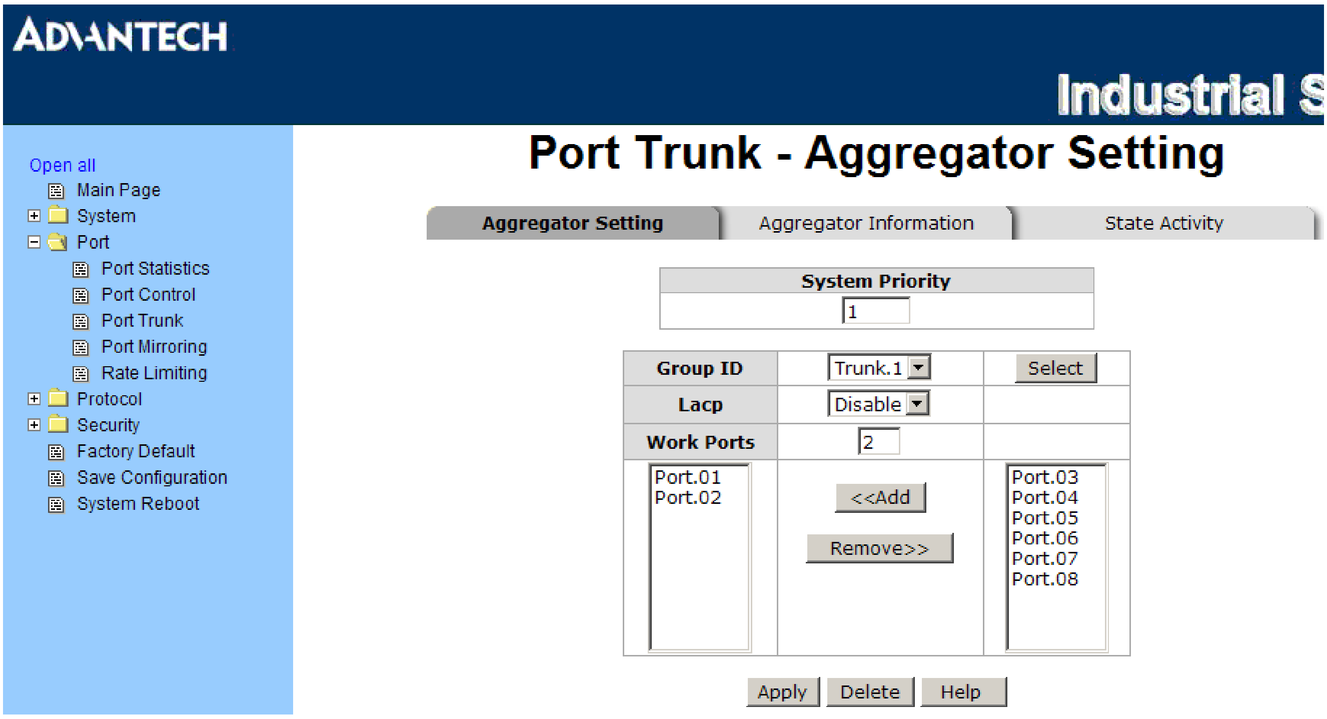
Figure 3.24: Port Control

Port Trunk

The Link Aggregation Control Protocol (LACP) provides a standardized means for exchanging information between Partner Systems on a link to allow their Link Aggregation Control instances to reach agreement on the identity of the Link Aggregation Group to which the link belongs, move the link to that Link Aggregation Group, and enable its transmission and reception functions in an orderly manner. Link aggregation lets you group up to 4 consecutive ports into two dedicated connections. This feature can expand bandwidth to a device on the network. LACP operation requires full-duplex mode, more detail information refers to IEEE 802.3ad.

Aggregator setting

- **System Priority:** a value used to identify the active LACP. The switch with the lowest value has the highest priority and is selected as the active LACP.
- **Group ID:** There are four trunk groups to provide configure. Choose the "Group ID" and click Select.
- **LACP:** If enable, the group is LACP dynamic trunk group. If disable, the group is static trunk group. All ports support LACP dynamic trunk group. If connecting to the device that also supports LACP, the LACP dynamic trunk group will be created automatically.
- **Work ports:** allows max four ports to be aggregated at the same time. With LACP dynamic trunk group, the exceed ports are standby and can be aggregated if work ports fail. If it is static trunk group, the number of ports must be the same as the group member ports.
- Select the ports to join the trunk group. Allows max four ports to be aggregated at the same time. Click Add button to add the port. To remove unwanted ports, select the port and click Remov button.
- If LACP enable, you can configure LACP Active/Passive status in each ports on State Activity page.
- Click Apply.
- Use Apply button to delete Trunk Group. Select the Group ID and click Delete button.

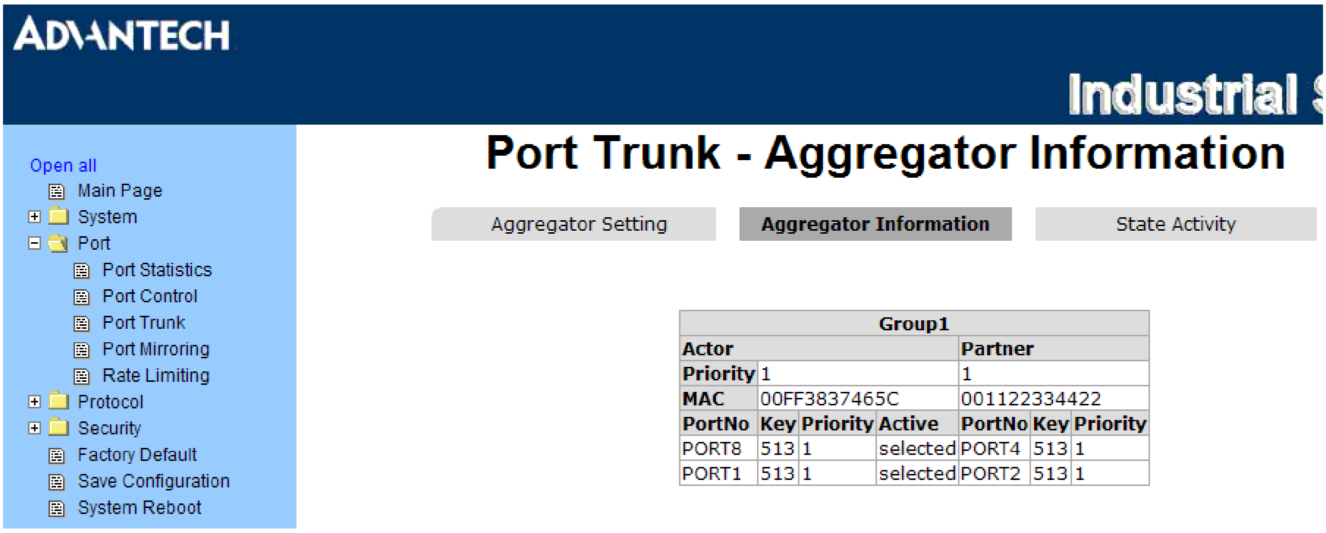


System Priority	1	
Group ID	Trunk.1	Select
Lacp	Disable	
Work Ports	2	
Port.01 Port.02		Port.03 Port.04 Port.05 Port.06 Port.07 Port.08

Figure 3.25: Aggregator Setting

Aggregator Information

When you have setup the aggregator setting with LACP disabled, you will see the local static trunk group information here.



Group1						
Actor				Partner		
Priority	1			1		
MAC	00FF3837465C			001122334422		
PortNo	Key	Priority	Active	PortNo	Key	Priority
PORT8	513	1	selected	PORT4	513	1
PORT1	513	1	selected	PORT2	513	1

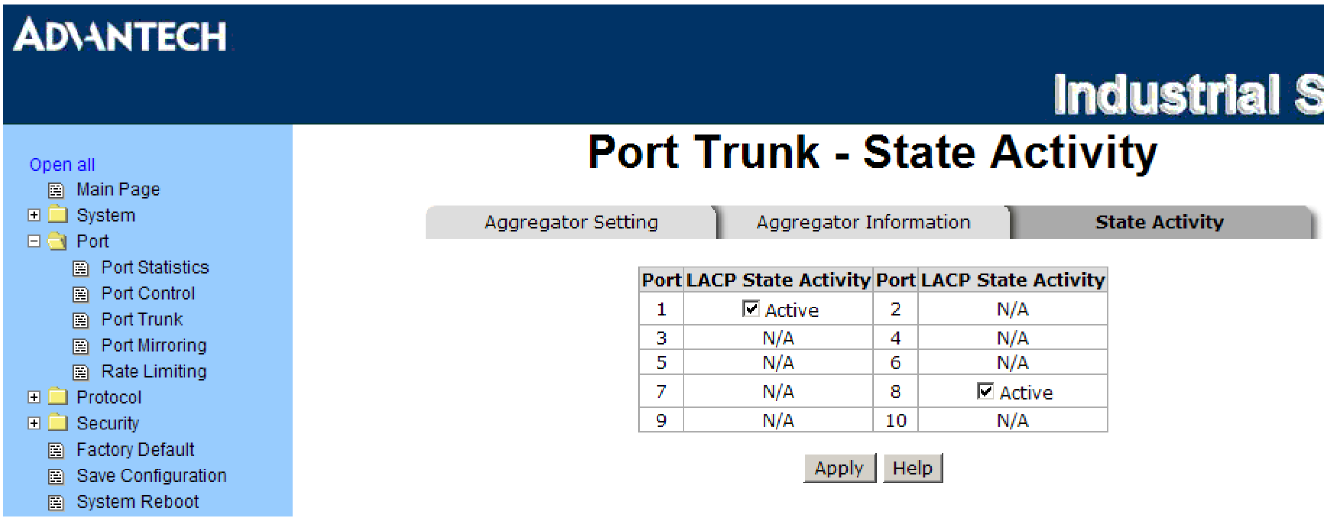
Figure 3.26: Aggregator Information

State Activity

When you had setup the LACP aggregator, you can configure port state activity. You can mark or un-mark the port. When you mark the port and click Apply button the port state activity will change to Active. Opposite is Passive.

- **Active:** The port automatically sends LACP protocol packets.
- **Passive:** The port does not automatically send LACP protocol packets, and responds only if it receives LACP protocol packets from the opposite device.

Note *A link having either two active LACP ports or one active port can perform dynamic LACP trunk.*
A link has two passive LACP ports will not perform dynamic LACP trunk because both ports are waiting for an LACP protocol packet from the opposite device.
If you are the active LACP's actor, after you have selected trunk port, the active status will be activated automatically.



Port Trunk - State Activity

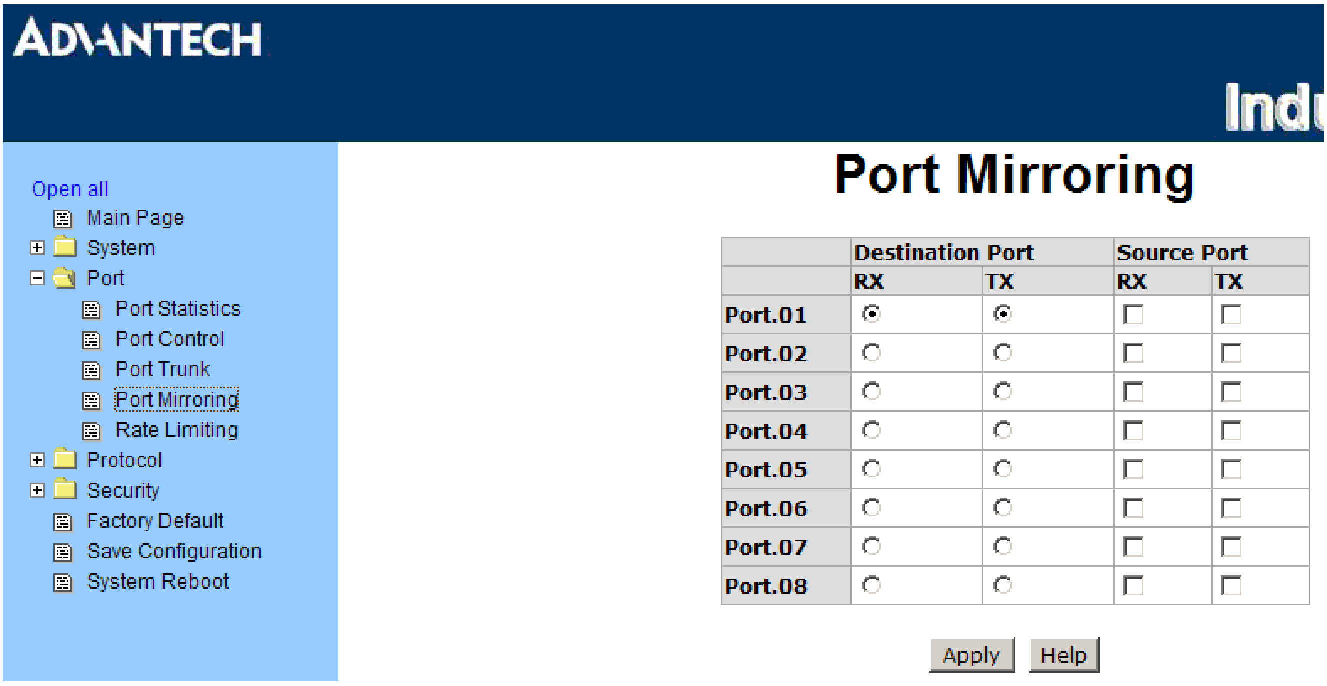
Port	LACP State Activity	Port	LACP State Activity
1	☑ Active	2	N/A
3	N/A	4	N/A
5	N/A	6	N/A
7	N/A	8	☑ Active
9	N/A	10	N/A

Figure 3.27: State Activity

Port Mirroring

The Port mirroring is a method for monitor traffic in switched networks. Traffic through ports can be monitored by one specific port. That means traffic goes in or out monitored (source) ports will be duplicated into mirror (destination) port.

- **Destination Port:** There is only one port can be selected to be destination (mirror) port for monitoring both RX and TX traffic which come from source port. Or, use one of two ports for monitoring RX traffic only and the other one for TX traffic only. User can connect mirror port to LAN analyzer or Netxray
- **Source Port:** The ports that user wants to monitor. All monitored port traffic will be copied to mirror (destination) port. User can select multiple source ports by checking the RX or TX check boxes to be monitored.
- And then, click Apply button.



Port Mirroring

	Destination Port		Source Port	
	RX	TX	RX	TX
Port.01	●	●	□	□
Port.02	○	○	□	□
Port.03	○	○	□	□
Port.04	○	○	□	□
Port.05	○	○	□	□
Port.06	○	○	□	□
Port.07	○	○	□	□
Port.08	○	○	□	□

Figure 3.28: Port Mirroring

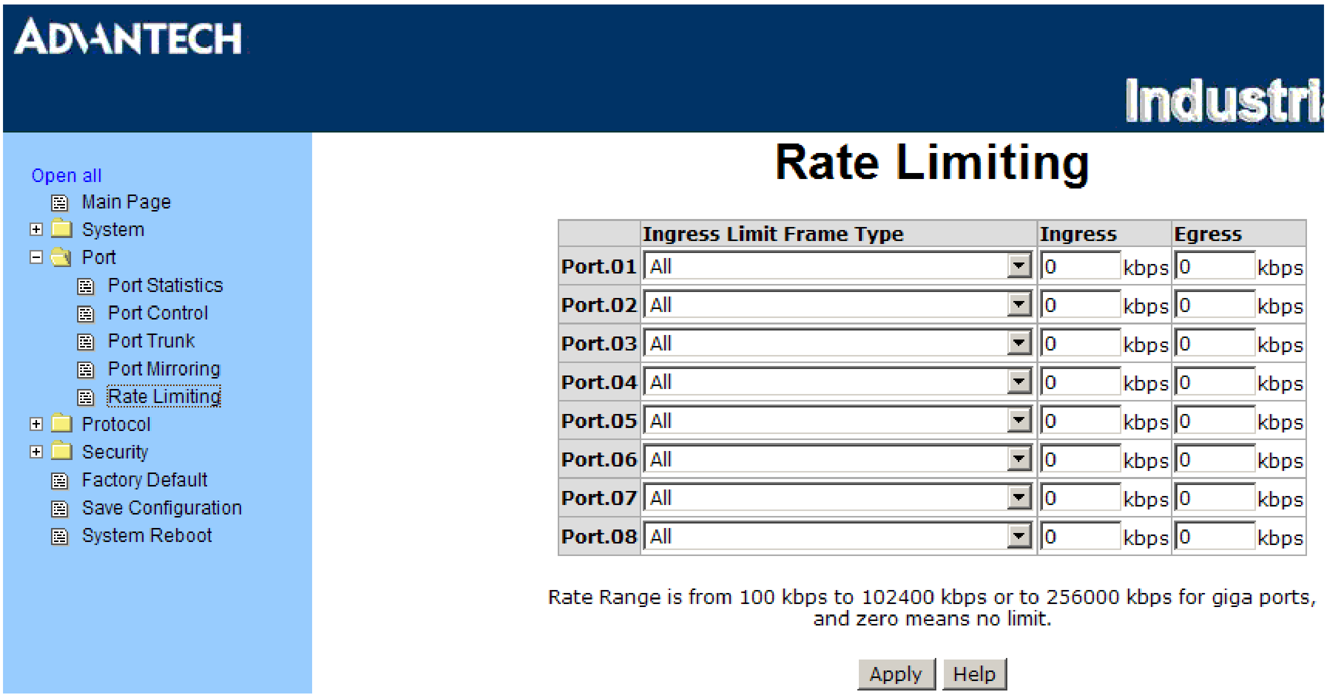
Rate Limiting

You can set up every port's bandwidth rate and frame limitation type.

- **Ingress Limit Frame type:** select the frame type that wants to filter. The frame types have 4 options for selecting: All, Broadcast/Multicast/Flooded Unicast, Broadcast/Multicast and Broadcast only. Broadcast/Multicast/Flooded Unicast, Broadcast/Multicast and Bbroadcast only types are only for ingress frames. The egress rate only supports All type.

- All the ports support port ingress and egress rate control. For example, assume port 1 is 10Mbps, users can set it's effective egress rate is 1Mbps, ingress rate is 500Kbps. The switch performs the ingress rate by packet counter to meet the specified rate

- **Ingress:** Enter the port effective ingress rate (The default value is "0")
- **Egress:** Enter the port effective egress rate (The default value is "0")
- And then, click Apply to apply the settings



Rate Limiting

	Ingress Limit Frame Type	Ingress	Egress
Port.01	All	0 kbps	0 kbps
Port.02	All	0 kbps	0 kbps
Port.03	All	0 kbps	0 kbps
Port.04	All	0 kbps	0 kbps
Port.05	All	0 kbps	0 kbps
Port.06	All	0 kbps	0 kbps
Port.07	All	0 kbps	0 kbps
Port.08	All	0 kbps	0 kbps

Rate Range is from 100 kbps to 102400 kbps or to 256000 kbps for giga ports, and zero means no limit.

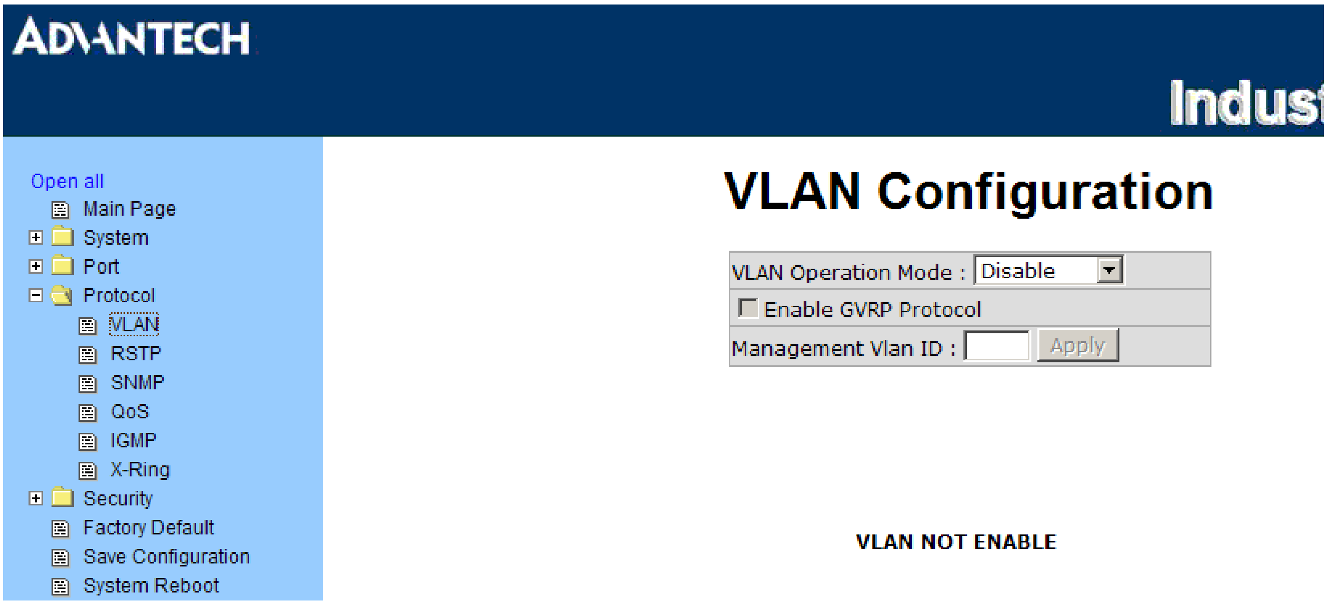
Figure 3.29: Rate Limiting

3.2.3 Protocol

VLAN configuration

A Virtual LAN (VLAN) is a logical network grouping that limits the broadcast domain, which would allow you to isolate network traffic, so only the members of the VLAN will receive traffic from the same members of VLAN. Basically, creating a VLAN from a switch is logically equivalent of reconnecting a group of network devices to another Layer 2 switch. However, all the network devices are still plugged into the same switch physically.

The industrial switch supports port-based and 802.1Q (tagged-based) VLAN. The default configuration of VLAN operation mode is "**Disable**".



VLAN Configuration

VLAN Operation Mode : Disable

□ Enable GVRP Protocol

Management Vlan ID :

VLAN NOT ENABLE

Figure 3.30: VLAN Configuration

VLAN configuration - Port-based VLAN

Packets can go among only members of the same VLAN group. Note all unselected ports are treated as belonging to another single VLAN. If the port-based VLAN enabled, the VLAN-tagging is ignored.

In order for an end station to send packets to different VLAN groups, it itself has to be either capable of tagging packets it sends with VLAN tags or attached to a VLAN-aware bridge that is capable of classifying and tagging the packet with different VLAN ID based on not only default PVID but also other information about the packet, such as the protocol.

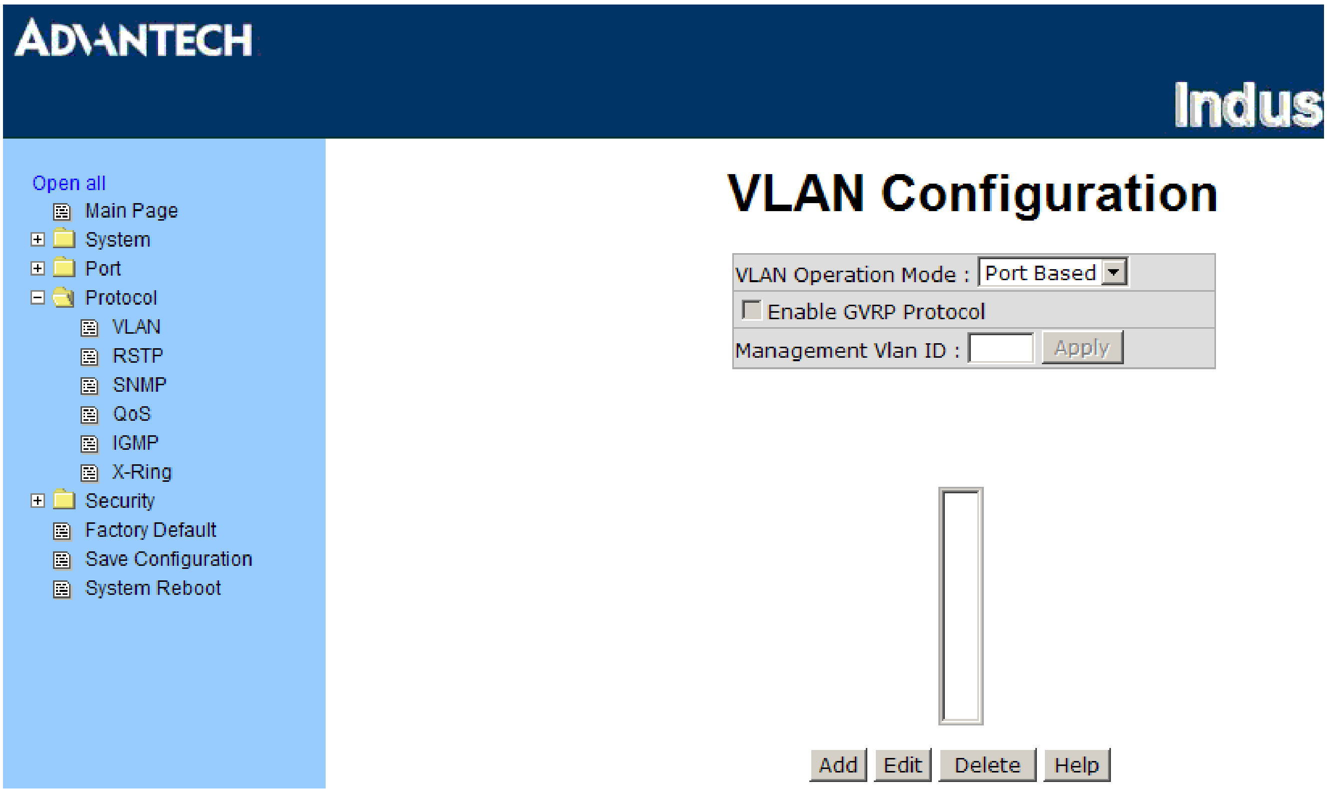
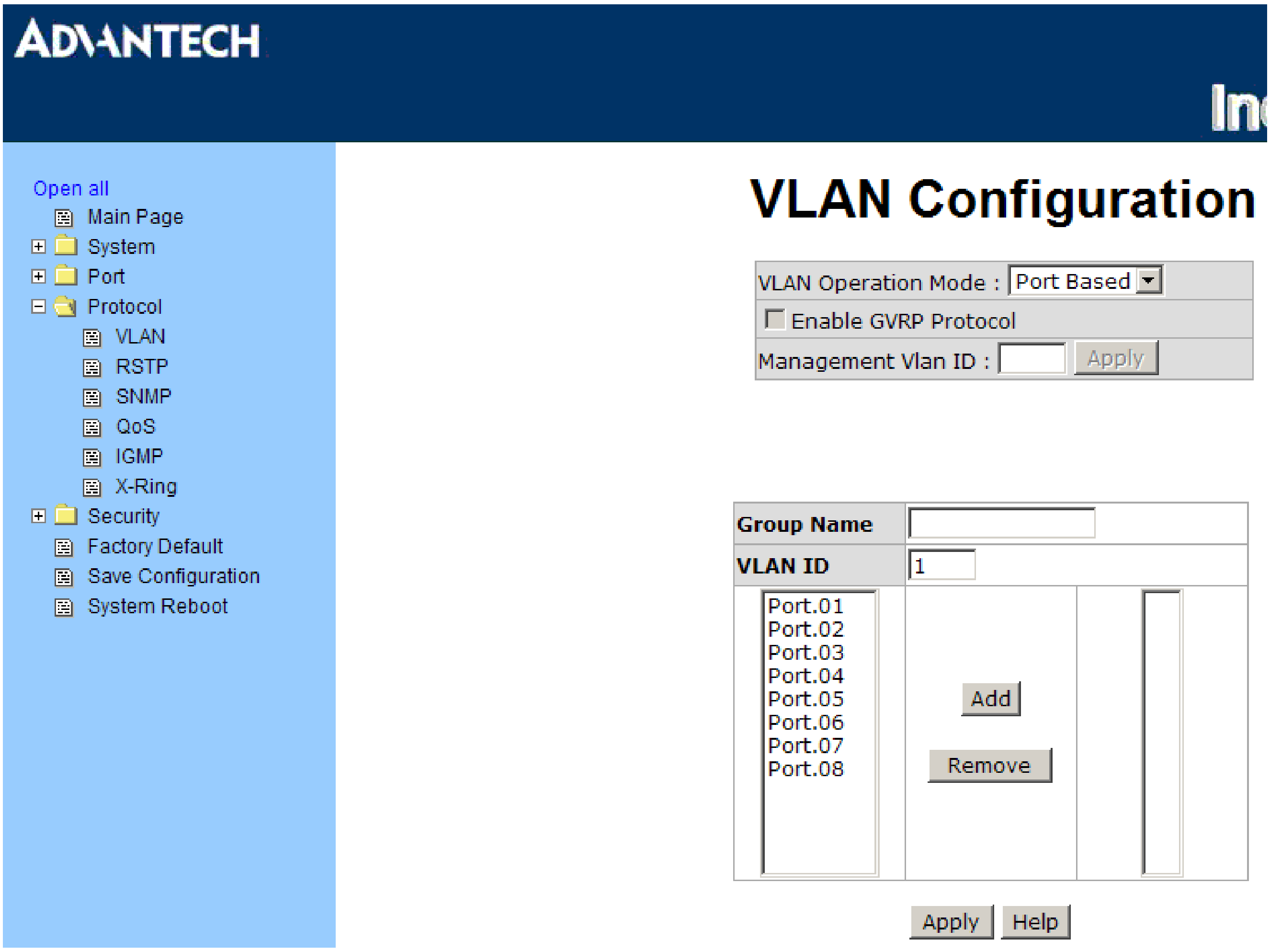


Figure 3.31: Port based mode

- Pull down the select item menu of VLAN Operation Mode, and select Port Based mode.
- Click Add to add a new VLAN group(The maximum VLAN group is up to 64 VLAN groups)
- Entering the VLAN name, group ID and grouping the members of VLAN group
- And then, click Apply



VLAN Configuration

VLAN Operation Mode : Port Based

☐ Enable GVRP Protocol

Management Vlan ID : [Apply]

Group Name	
VLAN ID	1

Port.01
Port.02
Port.03
Port.04
Port.05
Port.06
Port.07
Port.08

Figure 3.32: Port based mode-Add interface

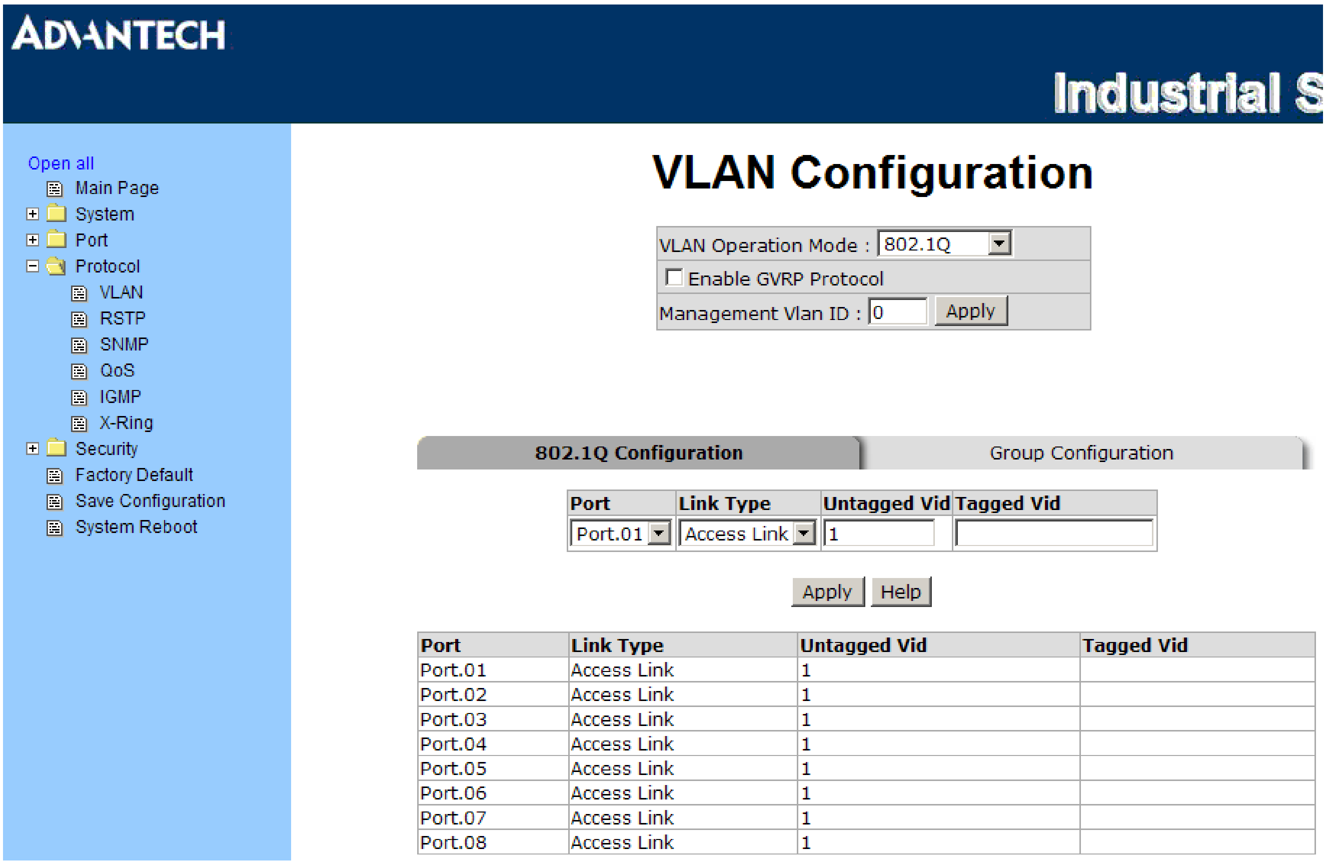
- You will see the VLAN displays.
- Use Delete button to delete unwanted VLAN.
- Use Edit button to modify existing VLAN group.

Note *Remember to execute the "**Save Configuration**" action, otherwise the new configuration will lose when switch power off.*

802.1Q VLAN

Tagged-based VLAN is an IEEE 802.1Q specification standard. Therefore, it is possible to create a VLAN across devices from different switch venders. IEEE 802.1Q VLAN uses a technique to insert a "tag" into the Ethernet frames. Tag contains a VLAN Identifier (VID) that indicates the VLAN numbers.
You can create Tag-based VLAN, and enable or disable GVRP protocol. There are 256 VLAN groups to provide configure. Enable 802.1Q VLAN, the all ports on the switch belong to default VLAN, VID is 1. The default VLAN can't be deleting.

GVRP allows automatic VLAN configuration between the switch and nodes. If the switch is connected to a device with GVRP enabled, you can send a GVRP request using the VID of a VLAN defined on the switch; the switch will automatically add that device to the existing VLAN.



VLAN Configuration

VLAN Operation Mode : 802.1Q

□ Enable GVRP Protocol

Management Vlan ID : 0 Apply

Port	Link Type	Untagged Vid	Tagged Vid
Port.01	Access Link	1	

Port	Link Type	Untagged Vid	Tagged Vid
Port.01	Access Link	1	
Port.02	Access Link	1	
Port.03	Access Link	1	
Port.04	Access Link	1	
Port.05	Access Link	1	
Port.06	Access Link	1	
Port.07	Access Link	1	
Port.08	Access Link	1	

Figure 3.33: 802.1Q VLAN Configuration

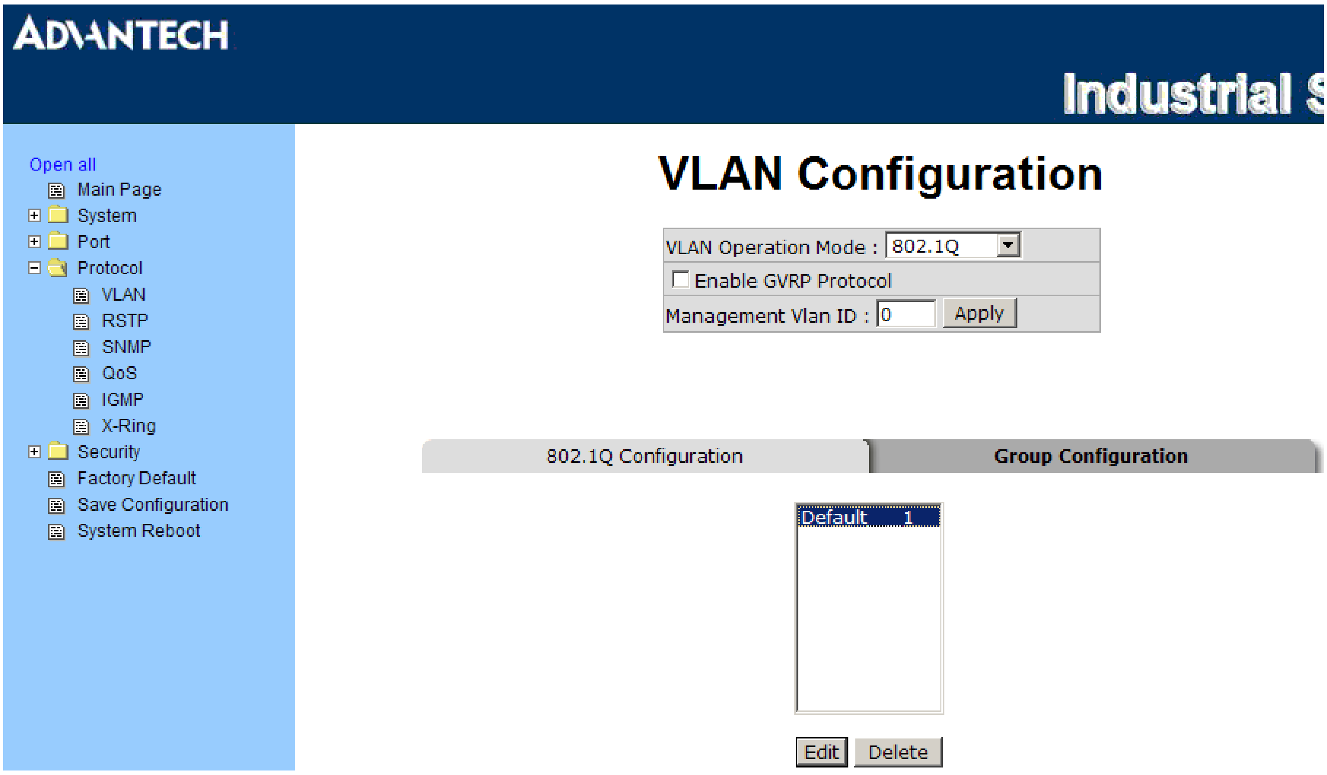
802.1Q Configuration

- Pull down the select item menu of VLAN Operation Mode, and select Port Based mode.
- **Enable GVRP Protocol:** mark the check box to enable GVRP protocol that allows network devices to dynamically exchange VLAN configuration information with other devices. If GVRP protocol is not enabled, user has to set the tagging information manually.
- Select the port that you want to configure.
- **Link Type:** there are 3 types of link type.
  - **Access Link:** single switch only, allow user to group ports by setting the same VID.
  - **Trunk Link:** extended application of **Access Link**, allows user to group ports by setting the same VID with 2 or more switches.
  - Hybrid Link: Both Access Link and Trunk Link are available.
- **Untagged VID:** assign the untagged frame VID.
- **Tagged VID:** assign the tagged frame VID.
- Click Apply

Group Configuration

Edit the existing VLAN Group.

- Select the VLAN group in the table list.
- Click Apply



VLAN Configuration

VLAN Operation Mode : 802.1Q

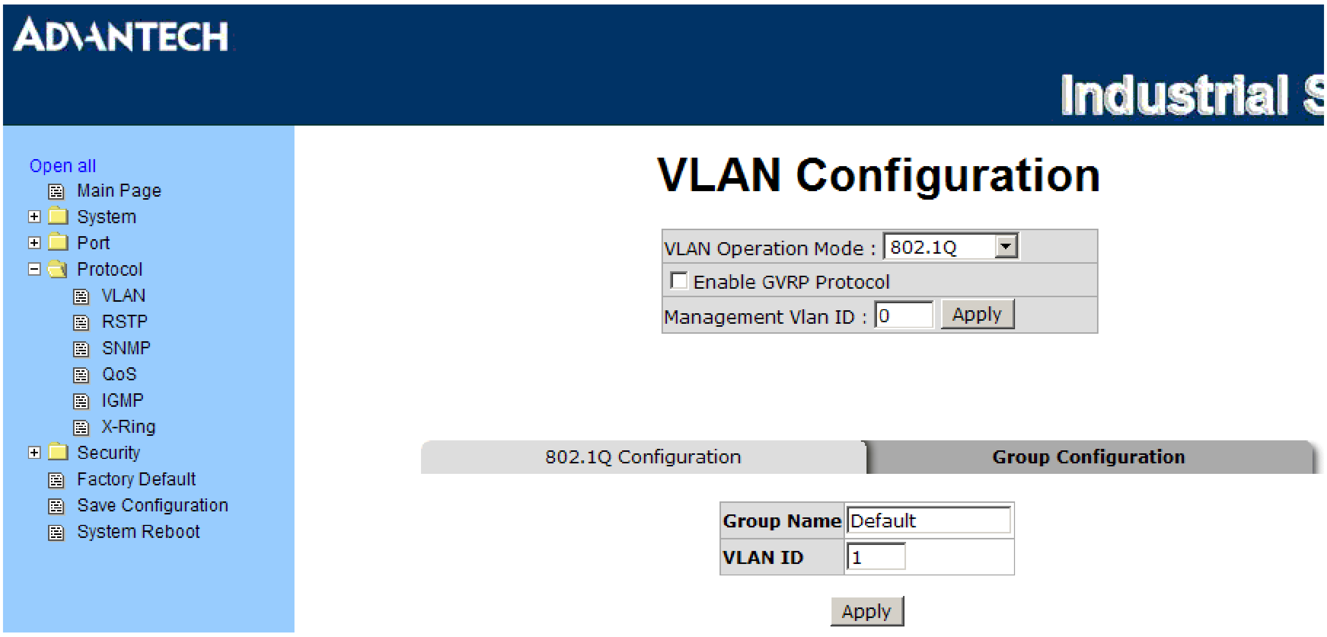
☐ Enable GVRP Protocol

Management Vlan ID : 0

Default 1

Figure 3.34: Edit Group Configuration interface

- You can Change the VLAN group name and VLAN ID.
- Click Apply.



VLAN Configuration

VLAN Operation Mode : 802.1Q

☐ Enable GVRP Protocol

Management Vlan ID : 0

Group Name	Default
VLAN ID	1

Figure 3.35: Apply Group Configuration interface

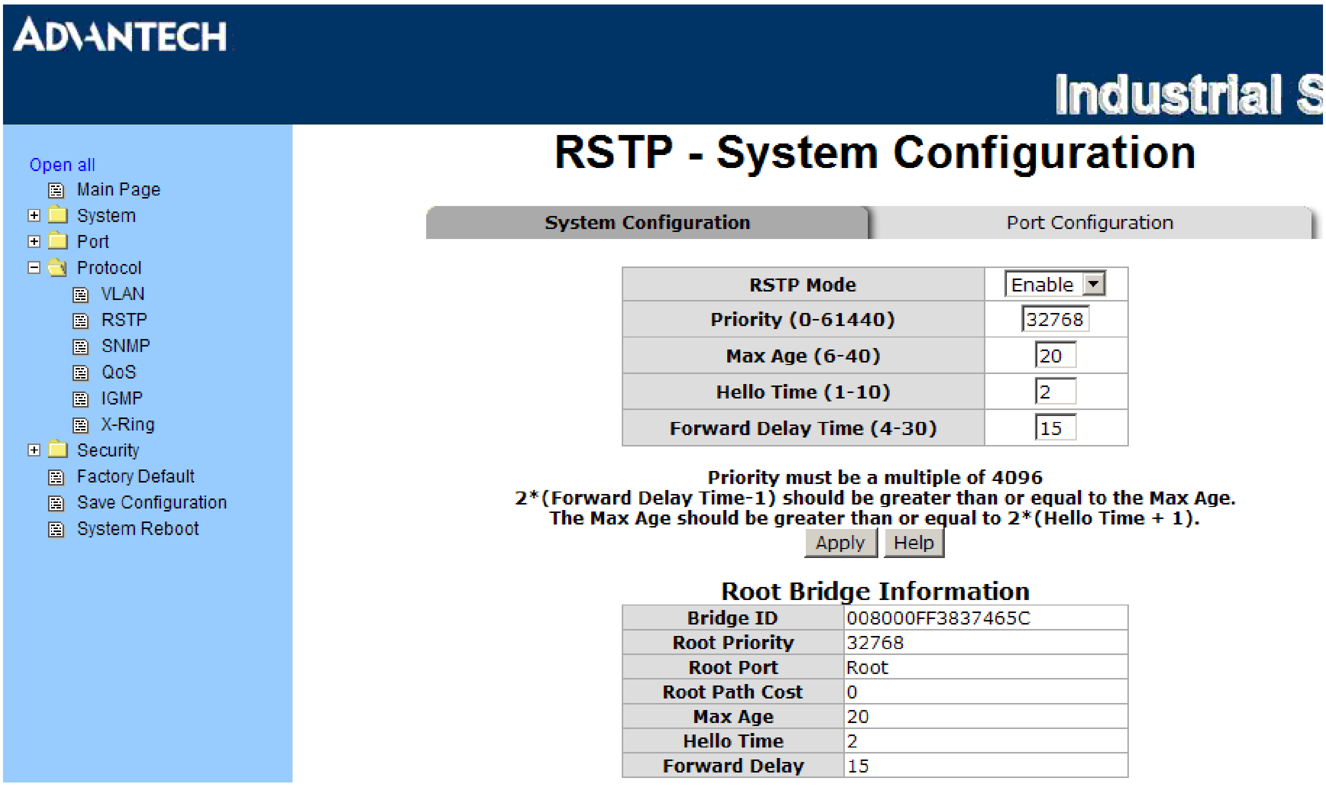
Rapid Spanning Tree

The Rapid Spanning Tree Protocol (RSTP) is an evolution of the Spanning Tree Protocol and provides for faster spanning tree convergence after a topology change. The system also supports STP and the system will auto detect the connected device that is running STP or RSTP protocol.

RSTP - System Configuration

- User can view spanning tree information about the Root Bridge
- User can modify RSTP state. After modification, click Apply button
  - ➢ **RSTP mode:** user must enable or disable RSTP function before configure the related parameters
  - ➢ **Priority (0-61440):** a value used to identify the root bridge. The bridge with the lowest value has the highest priority and is selected as the root. If the value changes, user must reboot the switch. The value must be multiple of 4096 according to the protocol standard rule
  - ➢ **Max Age (6-40):** the number of seconds a bridge waits without receiving Spanning-tree Protocol configuration messages before attempting a reconfiguration. Enter a value between 6 through 40
  - ➢ **Hello Time (1-10):** the time that controls switch sends out the BPDU packet to check RSTP current status. Enter a value between 1 through 10
  - ➢ **Forward Delay Time (4-30):** the number of seconds a port waits before changing from its Rapid Spanning-Tree Protocol learning and listening states to the forwarding state. Enter a value between 4 through 30

Note *Follow the rule to configure the MAX Age, Hello Time, and Forward Delay Time.* ***2 x (Forward Delay Time value –1) > = Max Age value >= 2 x (Hello Time value +1)***



RSTP - System Configuration

RSTP Mode	Enable
Priority (0-61440)	32768
Max Age (6-40)	20
Hello Time (1-10)	2
Forward Delay Time (4-30)	15

Priority must be a multiple of 4096
2*(Forward Delay Time-1) should be greater than or equal to the Max Age.
The Max Age should be greater than or equal to 2*(Hello Time + 1).

Root Bridge Information

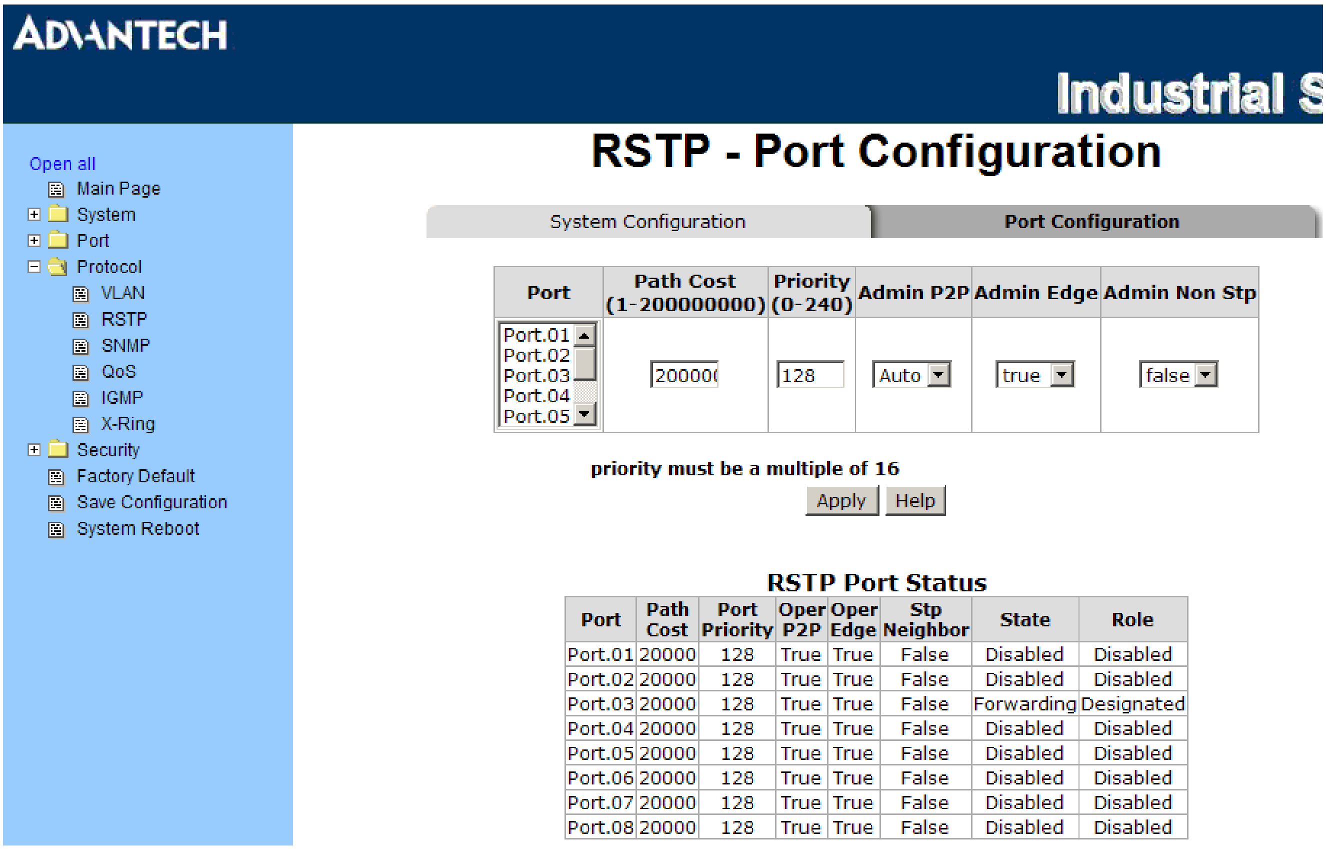
Bridge ID	008000FF3837465C
Root Priority	32768
Root Port	Root
Root Path Cost	0
Max Age	20
Hello Time	2
Forward Delay	15

Figure 3.36: RSTP System Configuration interface

RSTP - Port Configuration

You can configure path cost and priority of every port.

- Select the port in Port column.
- **Path Cost:** The cost of the path to the other bridge from this transmitting bridge at the specified port. Enter a number 1 through 200000000.
- **Priority:** Decide which port should be blocked by priority in LAN. Enter a number 0 through 240. The value of priority must be the multiple of 16.
- **P2P:** Some of the rapid state transactions that are possible within RSTP are dependent upon whether the port concerned can only be connected to exactly one other bridge (i.e. it is served by a point-to-point LAN segment), or can be connected to two or more bridges (i.e. it is served by a shared medium LAN segment). This function allows the P2P status of the link to be manipulated administratively. True is P2P enabling. False is P2P disabling.
- **Edge:** The port directly connected to end stations cannot create bridging loop in the network. To configure the port as an edge port, set the port to "True" status.
- **Non Stp:** The port includes the STP mathematic calculation. True is not including STP mathematic calculation. False is including the STP mathematic calculation.
- Click Apply .



RSTP - Port Configuration

Port	Path Cost (1-200000000)	Priority (0-240)	Admin P2P	Admin Edge	Admin Non Stp
Port.01 Port.02 Port.03 Port.04 Port.05	20000(	128	Auto	true	false

priority must be a multiple of 16

Apply Help

RSTP Port Status

Port	Path Cost	Port Priority	Oper P2P	Oper Edge	Stp Neighbor	State	Role
Port.01	20000	128	True	True	False	Disabled	Disabled
Port.02	20000	128	True	True	False	Disabled	Disabled
Port.03	20000	128	True	True	False	Forwarding	Designated
Port.04	20000	128	True	True	False	Disabled	Disabled
Port.05	20000	128	True	True	False	Disabled	Disabled
Port.06	20000	128	True	True	False	Disabled	Disabled
Port.07	20000	128	True	True	False	Disabled	Disabled
Port.08	20000	128	True	True	False	Disabled	Disabled

Figure 3.37: RSTP Port Configuration interface

SNMP Configuration

Simple Network Management Protocol (SNMP) is the protocol developed to manage nodes (servers, workstations, routers, switches and hubs etc.) on an IP network. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth. Network management systems learn of problems by receiving traps or change notices from network devices implementing SNMP.

System Configuration

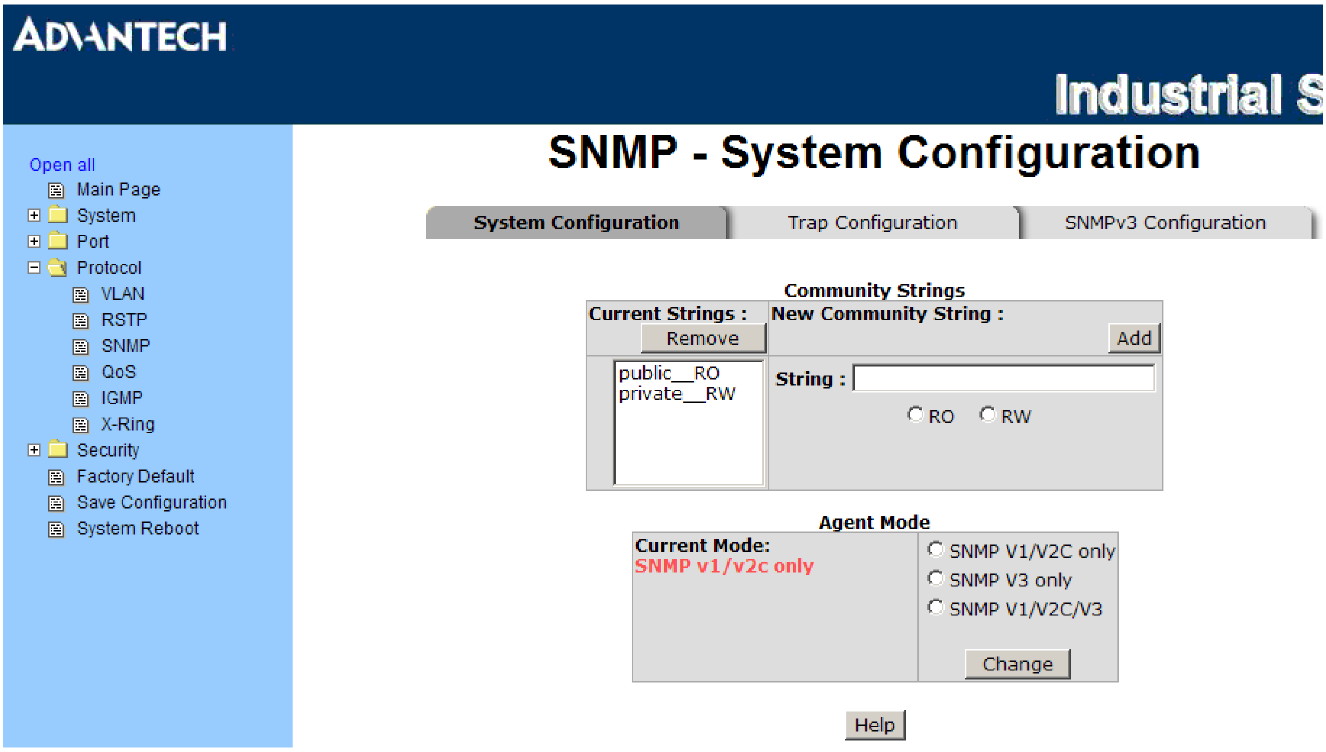
Community Strings

You can define new community string set and remove unwanted community string.

- **String:** Fill the name string.
- **RO:** Read only. Enables requests accompanied by this string to display MIB-object information.
- **RW:** Read write. Enables requests accompanied by this string to display MIB-object information and to set MIB objects.
- Click Add.
- To remove the community string, select the community string that you have defined and click Remove. You cannot edit the name of the default community string set.

Agent Mode

Select the SNMP version that you want to use it. And then click Change to switch to the selected SNMP version mode.



SNMP - System Configuration

Community Strings

Current Strings :

public__RO
private__RW

New Community String :

String :

○ RO ○ RW

Agent Mode

Current Mode:
SNMP v1/v2c only

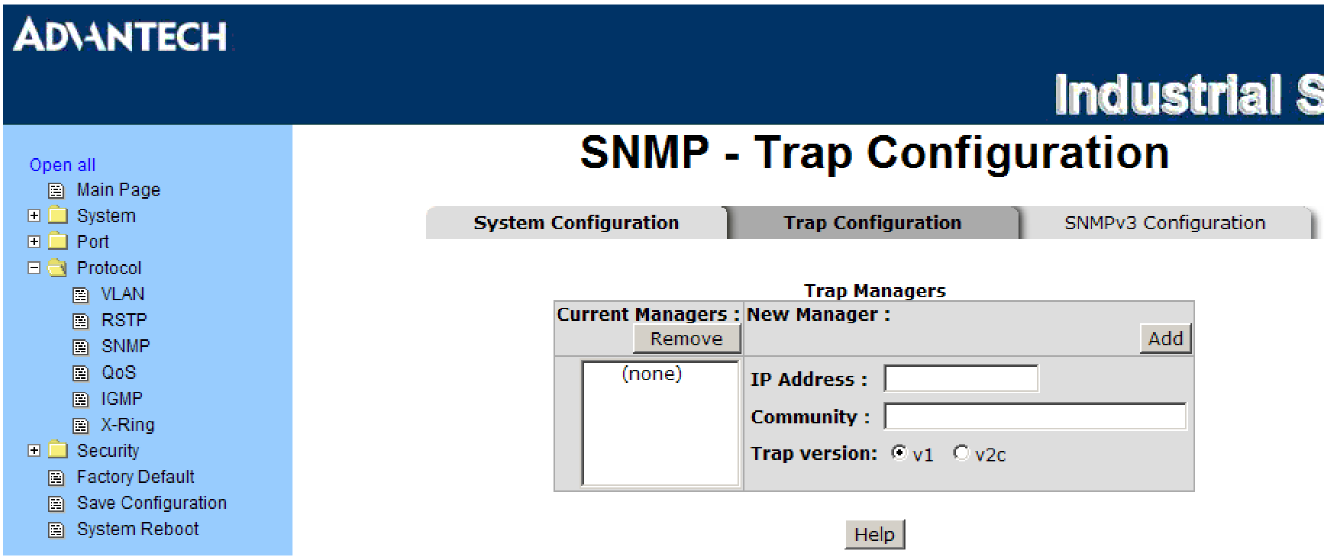
○ SNMP V1/V2C only
○ SNMP V3 only
○ SNMP V1/V2C/V3

Figure 3.38: SNMP System Configuration interface

Trap Configuration

A trap manager is a management station that receives traps, the system alerts generated by the switch. If no trap manager is defined, no traps will issue. Create a trap manager by entering the IP address of the station and a community string. To define management stations as trap manager and enter SNMP community strings and selects the SNMP version.

- **IP Address:** Enter the IP address of trap manager.
- **Community:** Enter the community string.
- **Trap Version:** Select the SNMP trap version type – v1 or v2c.
- Click Add .
- To remove the community string, select the community string that you have defined and click Remove . You cannot edit the name of the default community string set.



SNMP - Trap Configuration

Trap Managers

Current Managers :	New Manager :
(none)	IP Address :
	Community :
	Trap version: ● v1 ○ v2c

Figure 3.39: Trap Configuration interface

SNMPV3 Configuration

Configure the SNMP V3 function.

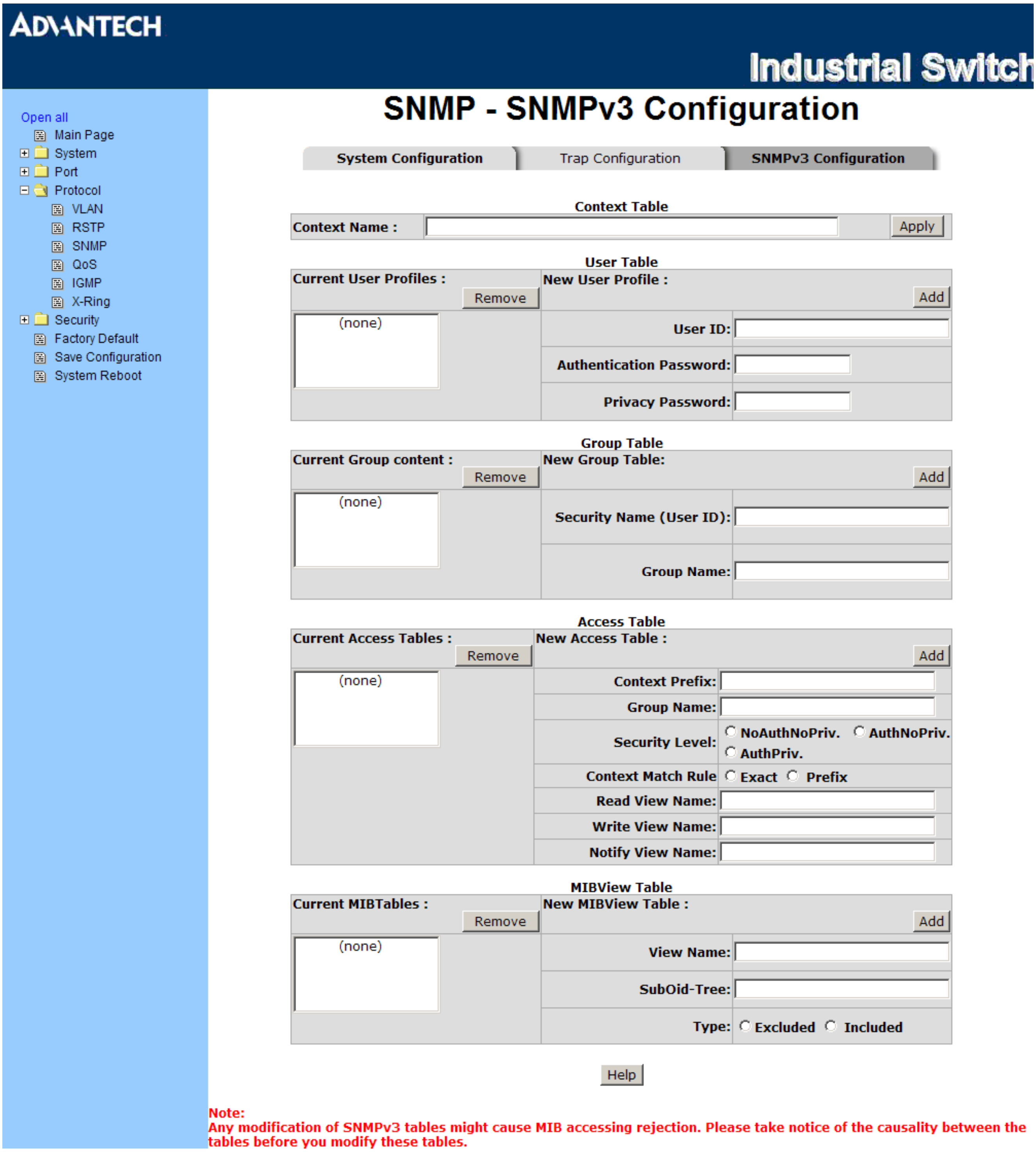
Context Table

Configure SNMP v3 context table. Assign the context name of context table. Click Add to add context name. Click Remove to remove unwanted context name.

User Profile

Configure SNMP v3 user table..

- **User ID:** set up the user name.
- **Authentication Password:** set up the authentication password.
- **Privacy Password:** set up the private password.
- Click Add to add context name.
- Click Remove to remove unwanted context name.



SNMP - SNMPv3 Configuration

Context Table

Context Name :

User Table

Current User Profiles :	New User Profile :
(none)	User ID:
	Authentication Password:
	Privacy Password:

Group Table

Current Group content :	New Group Table:
(none)	Security Name (User ID):
	Group Name:

Access Table

Current Access Tables :	New Access Table :
(none)	Context Prefix:
	Group Name:
	Security Level: ○ NoAuthNoPriv. ○ AuthNoPriv. ○ AuthPriv.
	Context Match Rule ○ Exact ○ Prefix
	Read View Name:
	Write View Name:
	Notify View Name:

MIBView Table

Current MIBTables :	New MIBView Table :
(none)	View Name:
	SubOid-Tree:
	Type: ○ Excluded ○ Included

Note:
Any modification of SNMPv3 tables might cause MIB accessing rejection. Please take notice of the causality between the tables before you modify these tables.

Figure 3.40: SNMP V3 Configuration interface

Group Table

Configure SNMP v3 group table.

- **Security Name (User ID):** Assign the user name that you have set up in user table.
- **Group Name:** Set up the group name.
- Click Add to add context name.
- Click Remove to remove unwanted context name.

Access Table

Configure SNMP v3 access table.

- **Context Prefix:** Set up the context name.
- **Group Name:** Set up the group.
- **Security Level:** Set up the access level.
- **Context Match Rule:** Select the context match rule.
- **Read View Name:** Set up the read view.
- **Write View Name:** Set up the write view.
- **Notify View Name:** Set up the notify view.
- Click Add to add context name.
- Click Remove to remove unwanted context name.

MIBview Table

Configure MIB view table.

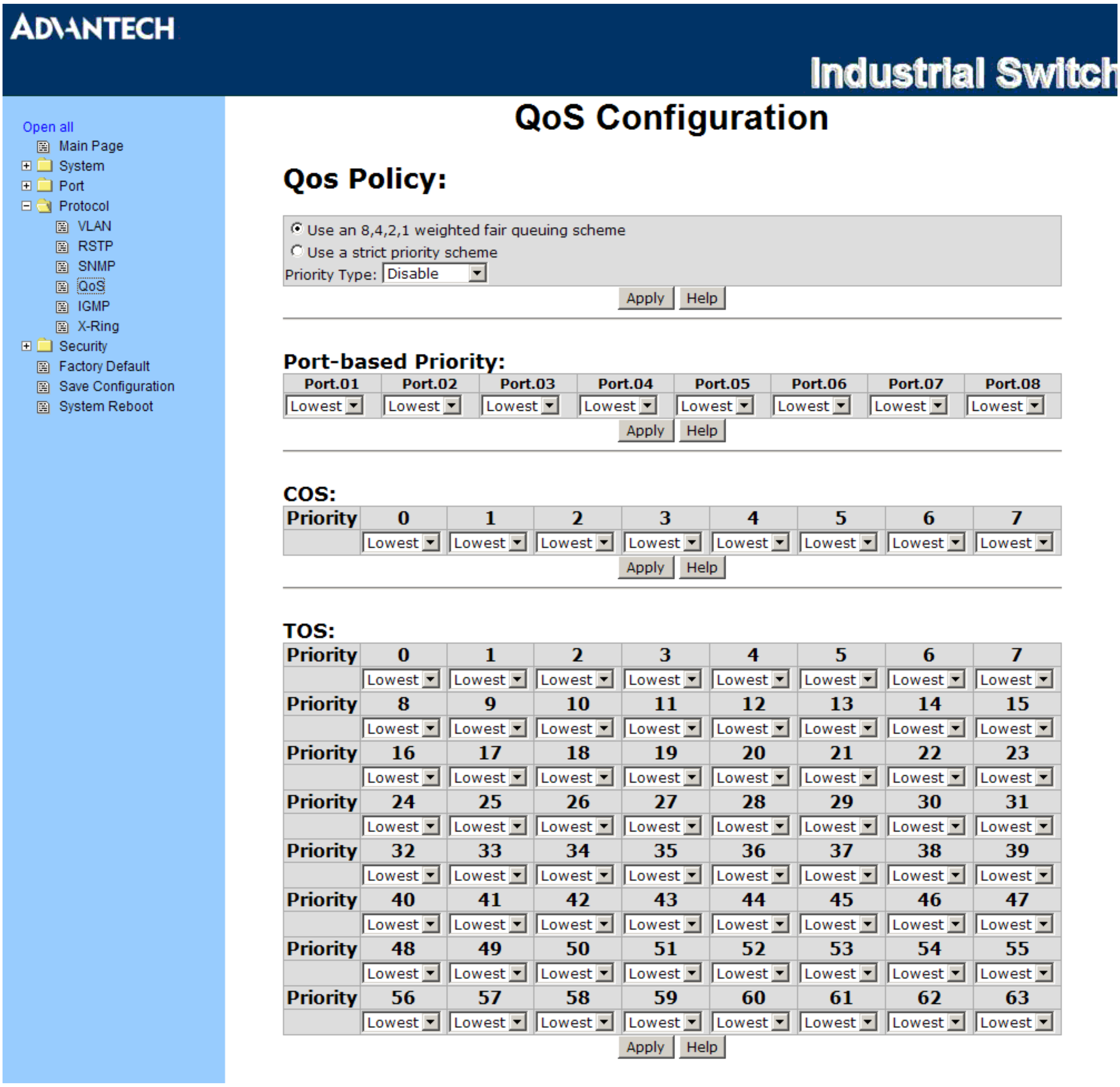
- **ViewName:** Set up the name.
- **Sub-Oid Tree:** Fill the Sub OID.
- **Type:** Select the type – exclude or included.
- Click Add to add context name.
- Click Remove to remove unwanted context name.

QoS Configuration

You can configure Qos policy and priority setting, per port priority setting, COS and TOS setting.

QoS Policy and Priority Type

- **Qos Policy:** select the Qos policy rule.
  - Use an 8,4,2,1 weighted fair queuing scheme: The switch will follow 8:4:2:1 rate to process priority queue from High to Lowest queue. For example, as the system processes 1 frames of the lowest queue, 2 frames of the low queue, 4 frames of the middle queue, and 8 frames of the high queue will be processed at the same time in accordance with the 8,4,2,1 policy rule.
  - Use a strict priority scheme: Always higher queue will be processed first, except higher queue is empty.
- **Priority Type:** there are 5 priority type selections available. Disable means no priority type is selected.
- **Port-base:** the port priority will follow the Port-base that you have assigned – High, middle, low, or lowest.
  - **COS only:** the port priority will only follow the COS priority that you have assigned.
  - **TOS only:** the port priority will only follow the TOS priority that you have assigned.
  - **COS first:** the port priority will follow the COS priority first, and then other priority rule.
  - **TOS first:** the port priority will follow the TOS priority first, and the other priority rule.
- Click Apply.



QoS Configuration

Qos Policy:

● Use an 8,4,2,1 weighted fair queuing scheme
○ Use a strict priority scheme
Priority Type: Disable

Port-based Priority:

Port.01	Port.02	Port.03	Port.04	Port.05	Port.06	Port.07	Port.08
Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest

COS:

Priority	0	1	2	3	4	5	6	7
	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest

TOS:

Priority	0	1	2	3	4	5	6	7
	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest
Priority	8	9	10	11	12	13	14	15
	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest
Priority	16	17	18	19	20	21	22	23
	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest
Priority	24	25	26	27	28	29	30	31
	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest
Priority	32	33	34	35	36	37	38	39
	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest
Priority	40	41	42	43	44	45	46	47
	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest
Priority	48	49	50	51	52	53	54	55
	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest
Priority	56	57	58	59	60	61	62	63
	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest

Figure 3.41: QoS Configuration interface

Port Base Priority

Configure per port priority level.

- **Port 1 ~ Port 10:** each port has 4 priority levels – High, Middle, Low, and Lowest.
- Click Apply.

COS Configuration

Set up the COS priority level.

- **COS priority:** Set up the COS priority level 0~7 –High, Middle, Low, Lowest.
- Click Apply.

TOS Configuration

Set up the TOS priority.

- **TOS priority:** the system provides 0~63 TOS priority level. Each level has 4 types of priority – high, middle, low, and lowest. The default value is “Lowest” priority for each level. When the IP packet is received, the system will check the TOS level value in the IP packet that has received. For example, user set the TOS level 25 is high. The port 1 is following the TOS priority policy only. When the port 1 packet received, the system will check the TOS value of the received IP packet. If the TOS value of received IP packet is 25(priority = high), and then the packet priority will have highest priority.
- Click Apply.

IGMP Configuration

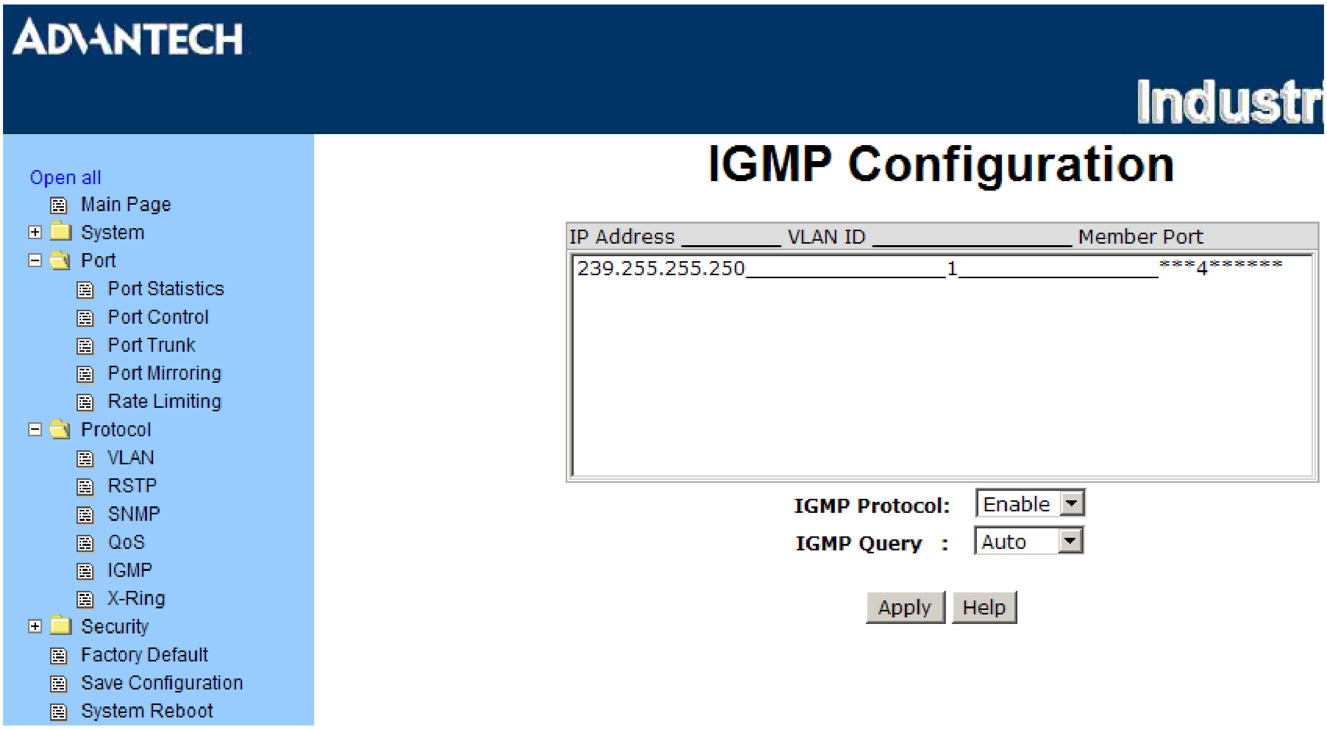
The Internet Group Management Protocol (IGMP) is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of the IP multicast specification, like ICMP for unicast connections. IGMP can be used for online video and gaming, and allows more efficient use of resources when supporting these uses.
IGMP have three fundamental types of message as follows:

Table 3.19: IGMP types

Message	Description
Query	A message sent from the querier (IGMP router or switch) asking for a response from each host belonging to the multicast group.
Report	A message sent by a host to the querier to indicate that the host wants to be or is a member of a given group indicated in the report message.
Leave Group	A message sent by a host to the querier to indicate that the host has quit being a member of a specific multicast group.

The switch support IP multicast, you can enable IGMP protocol on web management’s switch setting advanced page, then displays the IGMP snooping information. IP multicast addresses range are from 224.0.0.0 through 239.255.255.255.

- **IGMP Protocol:** Enable or disable the IGMP protocol.
- **IGMP Query:** Select the IGMP query function as Enable or Auto to set the switch as a querier for IGMP version 2 multicast network.
- Click Apply**.**



IGMP Configuration

IP Address	VLAN ID	Member Port
239.255.255.250	1	***4*******

IGMP Protocol: Enable

IGMP Query : Auto

Figure 3.42: IGMP Configuration interface

X-Ring

X-Ring provides a faster redundant recovery than Spanning Tree topology. The action is similar to STP or RSTP, but the algorithms not the same.

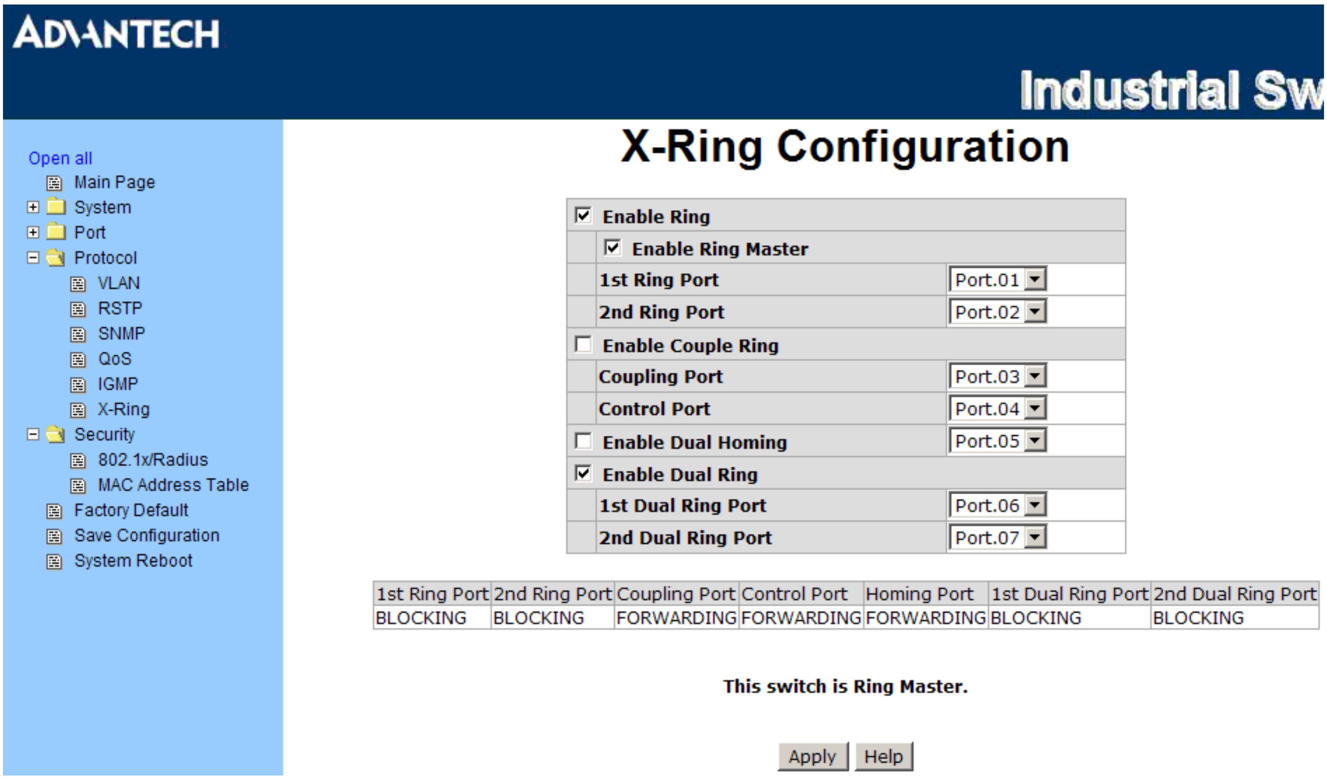
In the X-Ring topology, every switch should enable X-Ring function and assign two member ports in the ring. Only one switch in the X-Ring group would be set as a master switch, one of its path would be blocked, called backup port, and another port is called working port. Other switches in the X-Ring group are called working switches and their two member ports are called working ports. When the failure of network connection occurs, the backup port will automatically become a working port to recovery the failure.

The switch supports the function and interface for setting the switch as the ring master or slave mode. The ring master can negotiate and place command to other switches in the X-Ring group. If there are 2 or more switches in master mode, then software will select the switch with lowest MAC address number as the ring master. The X-Ring master ring mode will be enabled by the X-Ring configuration interface. Also, user can identify the switch as the ring master from the R.M. LED panel of the LED panel on the switch.

The system also supports the coupling ring that can connect 2 or more X-Ring group for the redundant backup function and dual homing function that prevent connection lose between X-Ring group and upper level/core switch.

- **Enable X-Ring**: To enable the X-Ring function. Marking the check box to enable the X-Ring function.
- **Enable Ring Master**: Mark the check box for enabling this machine to be a ring master.
- **1st & 2nd Ring Ports**: Pull down the selection menu to assign two ports as the member ports. 1st Ring Port is the working port and 2nd Ring Port is the backup port. When 1st Ring Port fails, the system will automatically upgrade the 2nd Ring Port to be the working port.
- **Enable Coupling Ring**: To enable the coupling ring function. Marking the check box to enable the coupling ring function.
- **Coupling port**: Assign the member port.
- **Control port**: Set the switch as the master switch in the coupling ring.
- **Enable Dual Homing**: Set up one of port on the switch to be the Dual Homing port. In an X-Ring group, maximum Dual Homing port is one. Dual Homing only work when the X-Ring function enable.

- **Enable Dual Ring**: When this check box is marked, the '**Enable Ring Master**' check box will then also be enabled by the system which means this equipment is assigned as the Ring Master. The Dual Ring differs from the Couple Ring in that it only needs a unit to form a redundant linking system of two rings.
- And then, click Apply to apply the configuration.



X-Ring Configuration

☑ Enable Ring	
☑ Enable Ring Master	
1st Ring Port	Port.01
2nd Ring Port	Port.02
☐ Enable Couple Ring	
Coupling Port	Port.03
Control Port	Port.04
☐ Enable Dual Homing	Port.05
☑ Enable Dual Ring	
1st Dual Ring Port	Port.06
2nd Dual Ring Port	Port.07

1st Ring Port	2nd Ring Port	Coupling Port	Control Port	Homing Port	1st Dual Ring Port	2nd Dual Ring Port
BLOCKING	BLOCKING	FORWARDING	FORWARDING	FORWARDING	BLOCKING	BLOCKING

This switch is Ring Master.

Figure 3.43: X-ring interface

Note *When the X-Ring function enable, user must disable the RSTP. The X-Ring function and RSTP function cannot exist at the same time.*
Remember to execute the "Save Configuration" action, otherwise the new configuration will lose when switch power off.

3.2.4 Security

In this section, you can configure 802.1x and MAC address table.

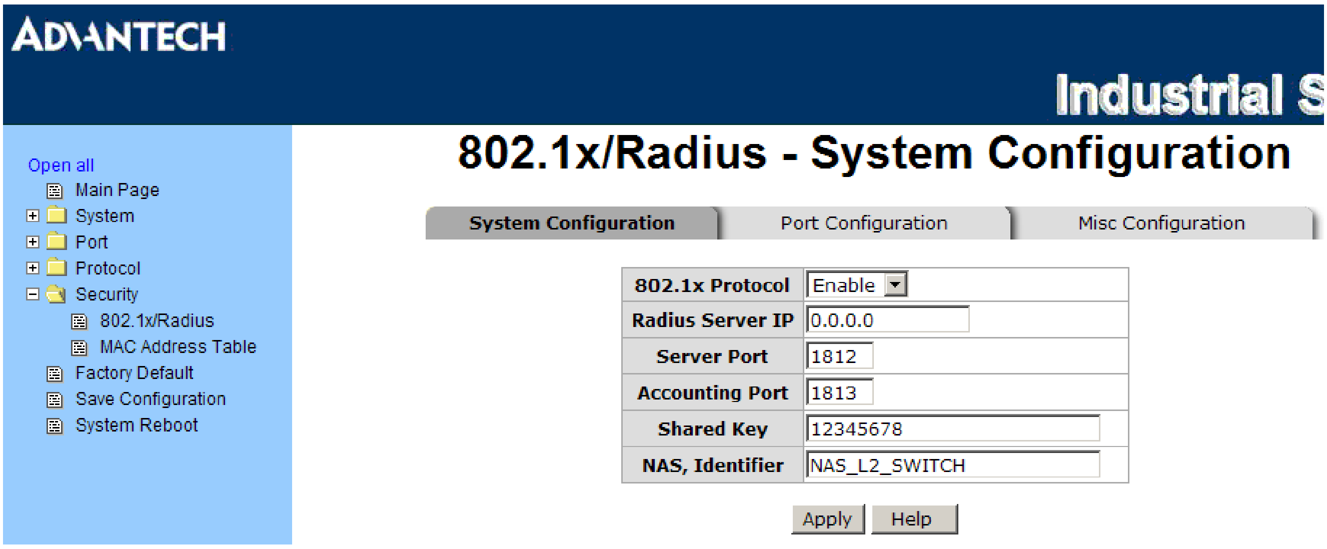
802.1X/Radius Configuration

802.1x is an IEEE authentication specification that allows a client to connect to a wireless access point or wired switch but prevents the client from gaining access to the Internet until it provides authority, like a user name and password that are verified by a separate server.

802.1X/Radius - System Configuration

After enabling the IEEE 802.1X function, you can configure the parameters of this function.

- **IEEE 802.1x Protocol:** .enable or disable 802.1x protocol.
- **Radius Server IP:** set the Radius Server IP address.
- **Server Port:** set the UDP destination port for authentication requests to the specified Radius Server.
- **Accounting Port:** set the UDP destination port for accounting requests to the specified Radius Server.
- **Shared Key:** set an encryption key for using during authentication sessions with the specified radius server. This key must match the encryption key used on the Radius Server.
- **NAS, Identifier:** set the identifier for the radius client.
- Click Apply .



802.1x/Radius - System Configuration

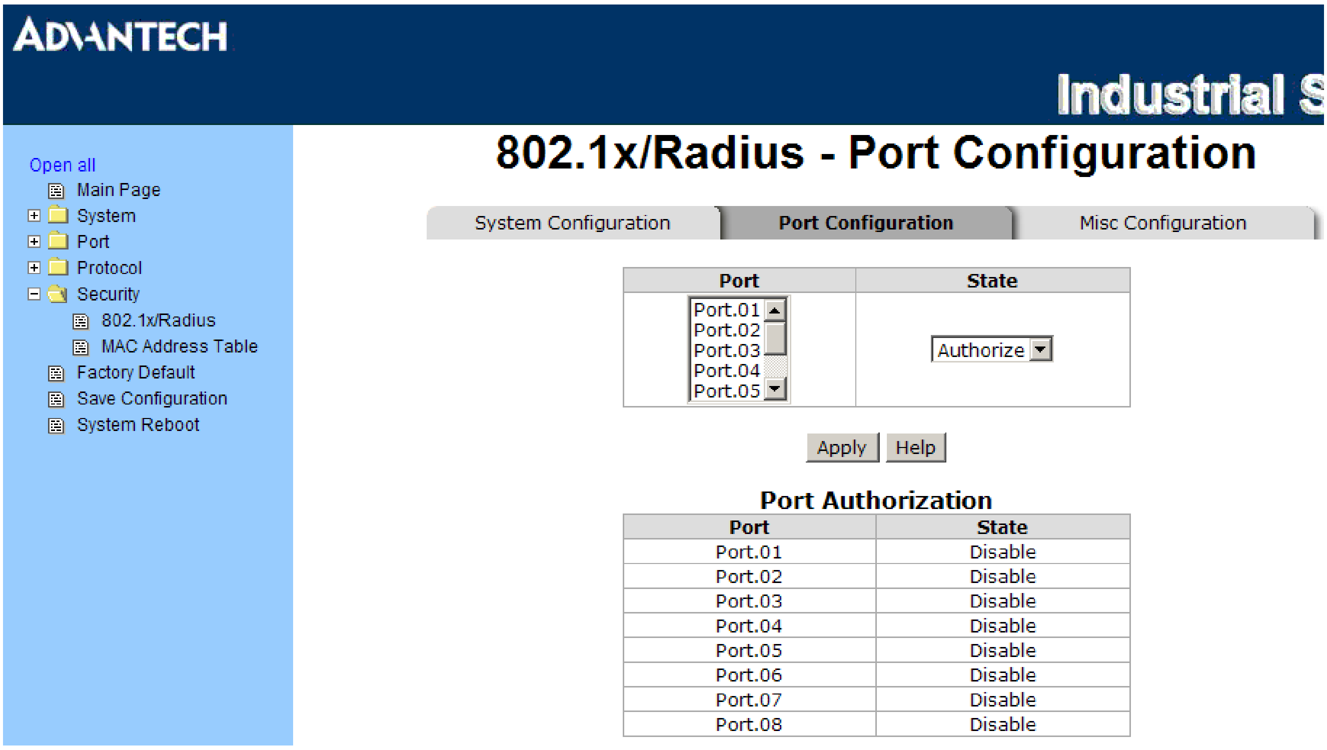
802.1x Protocol	Enable
Radius Server IP	0.0.0.0
Server Port	1812
Accounting Port	1813
Shared Key	12345678
NAS, Identifier	NAS_L2_SWITCH

Figure 3.44: 802.1x/Radius System Configuration interface

802.1x/Radius - Port Configuration

You can configure 802.1x authentication state for each port. The State provides Disable, Accept, Reject and Authorize. Use “Space” key change the state value.

- **Reject:** the specified port is required to be held in the unauthorized state.
- **Accept:** the specified port is required to be held in the Authorized state.
- **Authorized:** the specified port is set to the Authorized or Unauthorized state in accordance with the outcome of an authentication exchange between the Supplicant and the authentication server.
- **Disable:** The specified port is required to be held in the Authorized state
- Click Apply .



802.1x/Radius - Port Configuration

Port	State
Port.01 Port.02 Port.03 Port.04 Port.05	Authorize

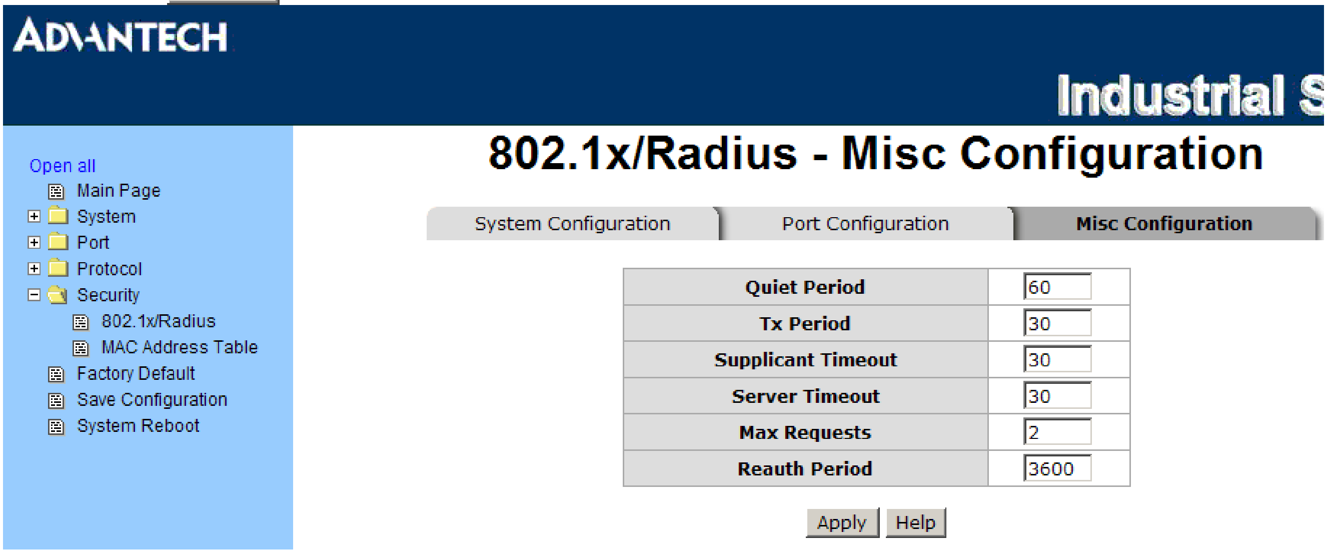
Port Authorization

Port	State
Port.01	Disable
Port.02	Disable
Port.03	Disable
Port.04	Disable
Port.05	Disable
Port.06	Disable
Port.07	Disable
Port.08	Disable

Figure 3.45: 802.1x/Radius - Port Setting interface

802.1X/Radius - Misc Configuration

- **Quiet Period:** set the period during which the port doesn’t try to acquire a supplicant.
- **TX Period:** set the period the port wait for retransmit next EAPOL PDU during an authentication session.
- **Supplicant Timeout:** set the period of time the switch waits for a supplicant response to an EAP request.
- **Server Timeout:** set the period of time the switch waits for a server response to an authentication request.
- **Max Requests:** set the number of authentication that must time-out before authentication fails and the authentication session ends.
- **Reauth period:** set the period of time after which clients connected must be re-authenticated.
- Click Apply .



802.1x/Radius - Misc Configuration

Quiet Period	60
Tx Period	30
Supplicant Timeout	30
Server Timeout	30
Max Requests	2
Reauth Period	3600

Figure 3.46: 802.1x/Radius - Misc Configuration interface

MAC Address Table

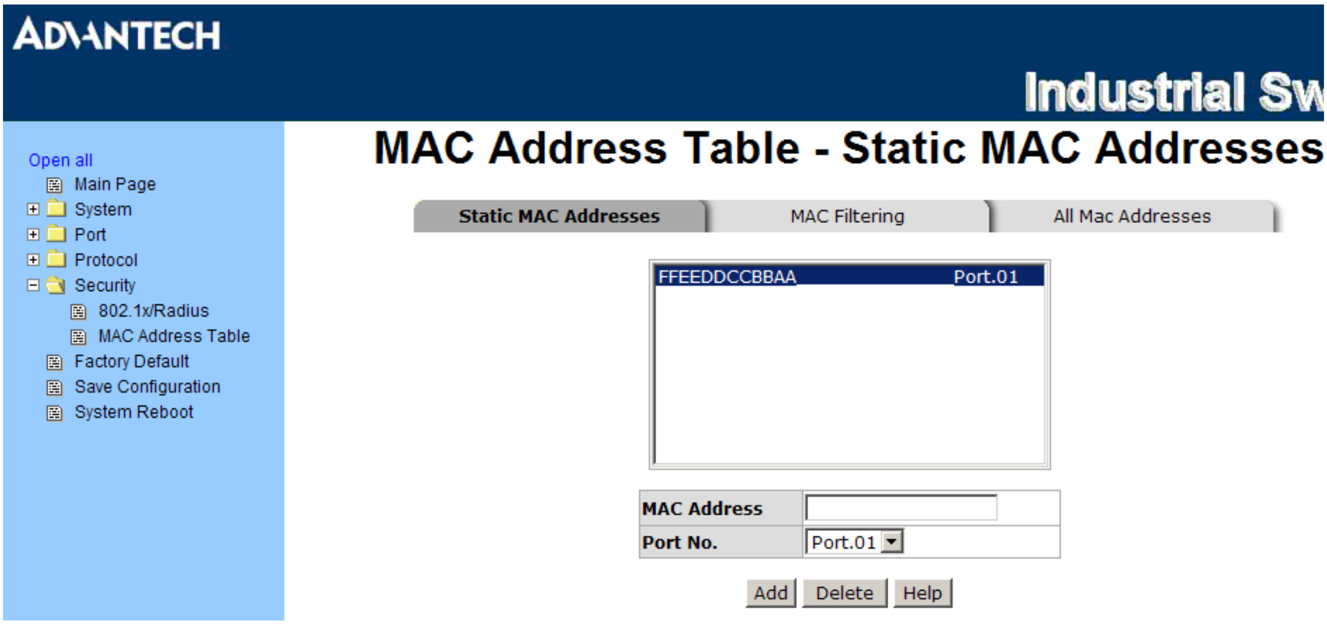
Use the MAC address table to ensure the port security.

You can add a static MAC address; it remains in the switch's address table, regardless of whether the device is physically connected to the switch. This saves the switch from having to re-learn a device's MAC address when the disconnected or powered-off device is active on the network again. You can add / modify / delete a static MAC address.

MAC Address Table - Static MAC Address

You can add static MAC address in the switch MAC table here.

- **MAC Address:** Enter the MAC address of the port that should permanently forward traffic, regardless of the device network activity.
- **Port No.:** pull down the selection menu to select the port number.
- Click Add .
- If you want to delete the MAC address from filtering table, select the MAC address and click Delete .



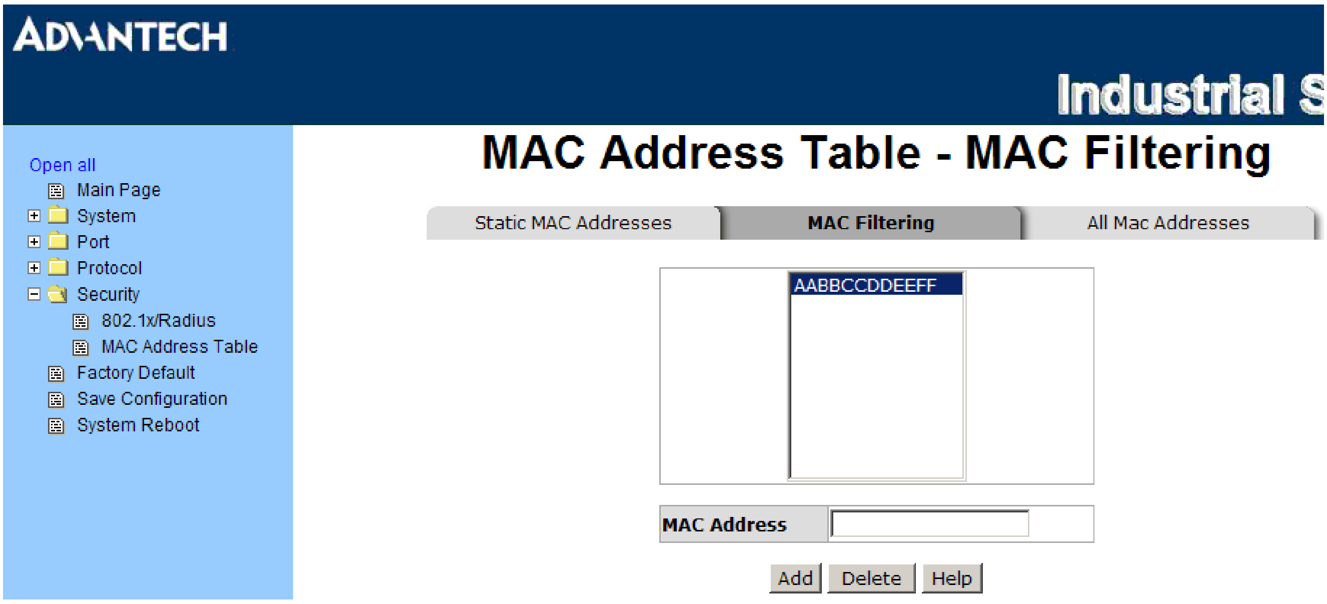
FFEEDDCCBBAA Port.01

MAC Address	
Port No.	Port.01

Figure 3.47: Static MAC Addresses interface

MAC Address Table - MAC Filtering

By filtering MAC address, the switch can easily filter pre-configure MAC address and reduce the un-safety. You can add and delete filtering MAC address.



MAC Address Table - MAC Filtering

AABBCCDDEEFF

MAC Address:

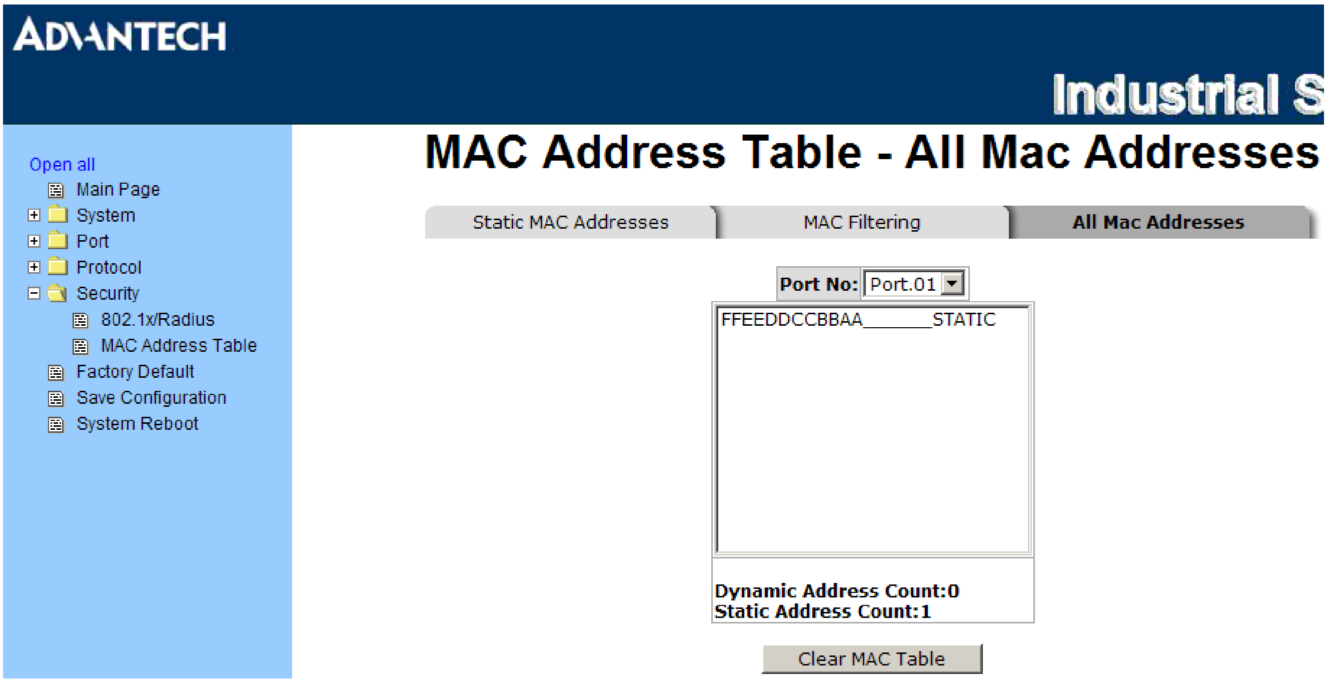
Figure 3.48: MAC Filtering interface

- MAC Address: Enter the MAC address that you want to filter.
- Click Add .
- If you want to delete the MAC address from filtering table, select the MAC address and click Delete .

MAC Address Table - All MAC Addresses

You can view the port that connected device's MAC address and related devices' MAC address.

- Select the port.
- The selected port of static MAC address information will be displayed here.
- Click Clear MAC Table to clear the current port static MAC address information on screen.



MAC Address Table - All Mac Addresses

Port No: Port.01

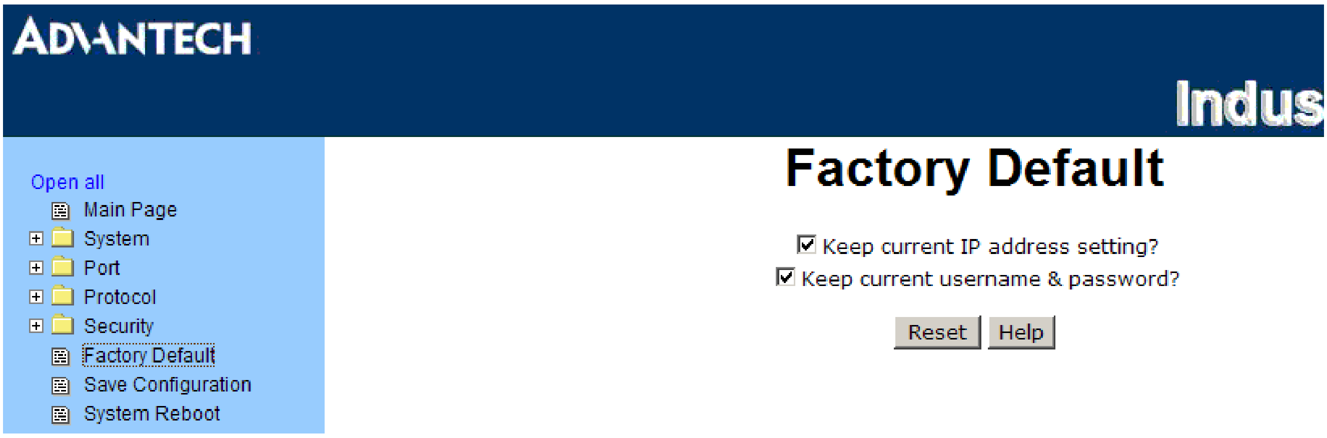
FFEEDDCCBBAA_______STATIC

Dynamic Address Count:0
Static Address Count:1

Figure 3.49: All MAC Address interface

Factory Default

Reset switch to default configuration. Click Reset to reset all configurations to the default value.



Factory Default

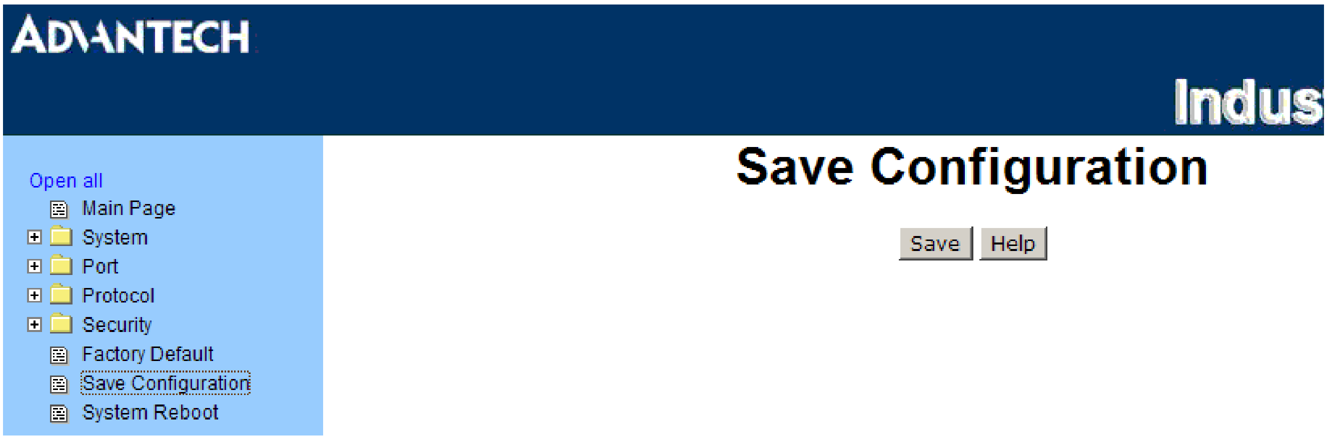
☑ Keep current IP address setting?

☑ Keep current username & password?

Figure 3.50: Factory Default interface

Save Configuration

Save all configurations that you have made in the system. To ensure the all configuration will be saved. Click Save to save the all configuration to the flash memory.

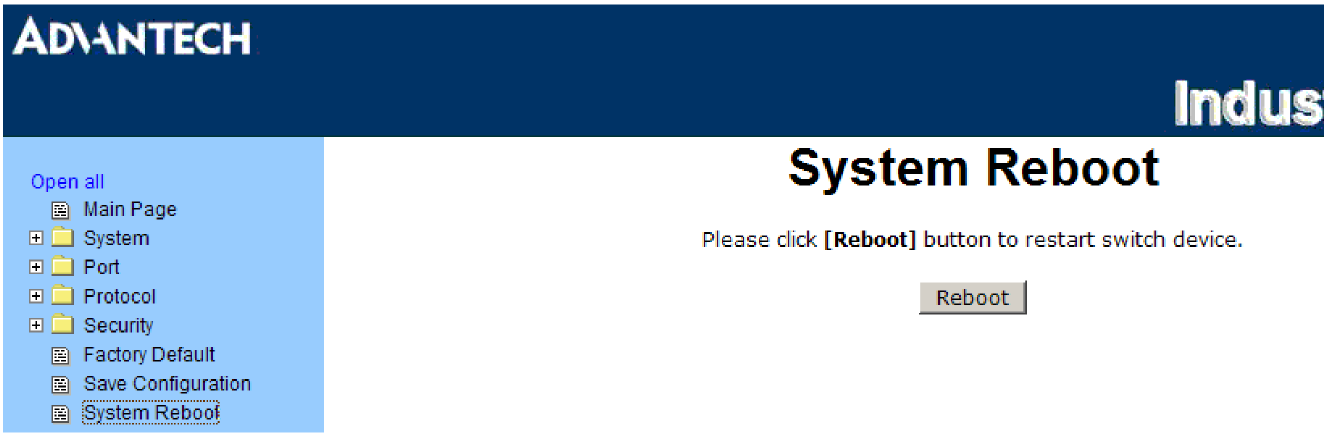


Save Configuration

Figure 3.51: Save Configuration interface

System Reboot

Reboot the switch in software reset. Click Reboot to reboot the system.



System Reboot

Please click **[Reboot]** button to restart switch device.

Figure 3.52: System Reboot interface

CHAPTER 4

Troubleshooting

Chapter 4 Troubleshooting

Verify that is using the right power cord/adapter (+12~48V$_{DC}$), please don't use the power adaptor with DC output voltage higher than 48 V, or it will burn this converter down.

Select the proper UTP cable to construct user network. Please check that is using the right cable. Use Unshielded Twisted-Pair (UTP) or Shielded Twisted-Pair (STP) cable for RJ-45 connections: 100 Category 3, 4 or 5 cable for 10 Mbps connections or 100 Category 5 cable for 100 Mbps connections. Also, be sure that the length of any twisted-pair connection does not exceed 100 meters (328 feet).

Diagnosing LED Indicators

The switch can be easily monitored through panel indicators, which describes common problems user may encounter and where user can find possible solutions, to assist in identifying.

If the power indicator does not light up when the power cord is plugged in, user may have a problem with power cord. Then check for loose power connections, power losses or surges at power outlet. If user still cannot resolve the problem, contact the local dealer for assistance.

If the Industrial switch LED indicators are normal and the connected cables are correct but the packets still cannot transmit, please check your system's Ethernet devices configuration or status.

APPENDIX A

Pin Assignment & Wiring

Appendix A   Pin Assignment & Wiring

It is suggested to adopt ELA/TIA as the wiring of the RJ-45.

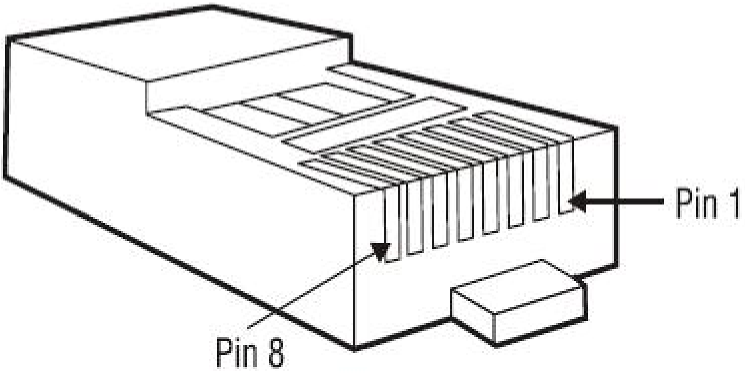
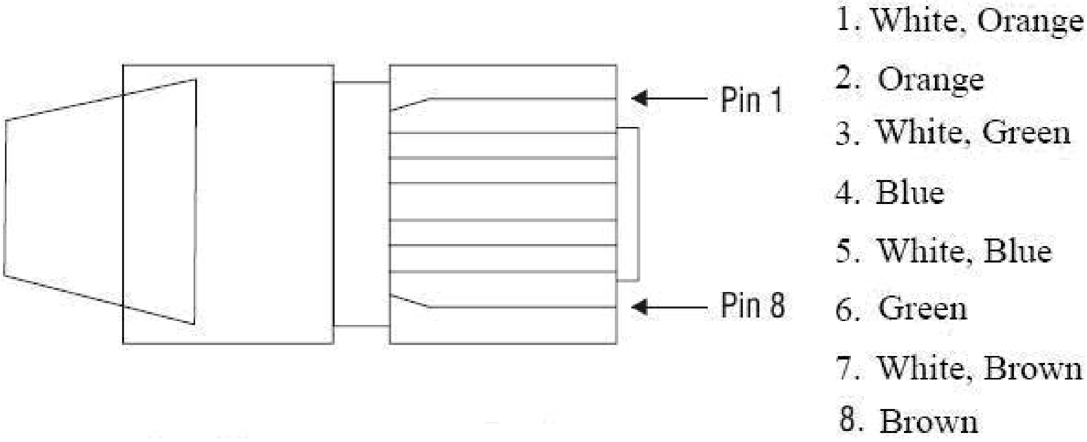
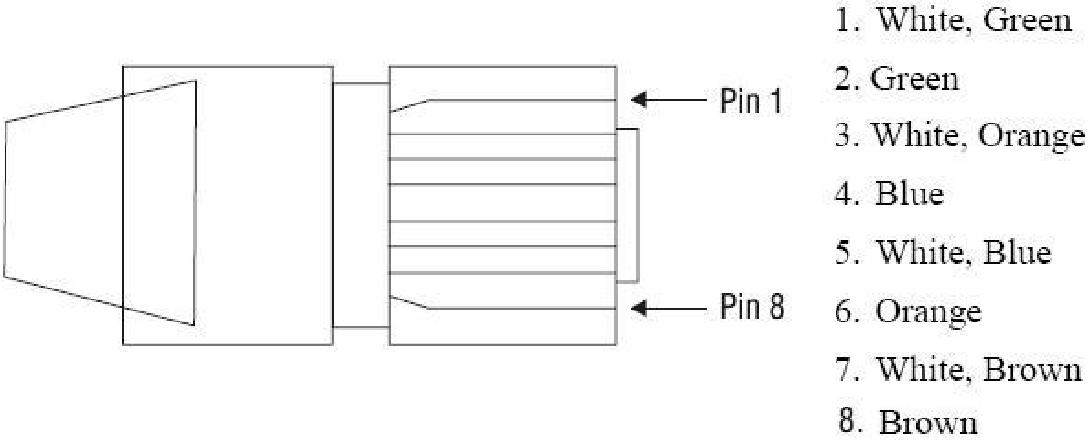


Figure A.1: RJ-45 Pin Assignment



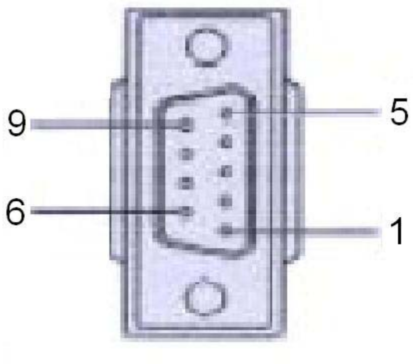
1. White, Orange
2. Orange
3. White, Green
4. Blue
5. White, Blue
6. Green
7. White, Brown
8. Brown

Figure A.2: EIA/TIA-568B



1. White, Green
2. Green
3. White, Orange
4. Blue
5. White, Blue
6. Orange
7. White, Brown
8. Brown

Figure A.3: EIA/TIA-568A



DB 9-pin Female

Figure A.4: DB 9-pin female connector

DB9 Connector	RJ-45 Connector
NC	1 Orange/White
2	2 Orange
3	3 Green/White
NC	4 Blue
5	5 Blue/White
NC	6 Green
NC	7 Brown/White
NC	8 Brown

APPENDIX B

Compatible SFP Modules

Appendix B Compatible SFP Modules

The table below shows compatible SFP modules for EKI-7758F.

Item	Brand	Part Number	Mode	Transmission Distance
1	AVAGO	AFBR-5710PZ	Multi-mode	550m
2	APAC	LM28-C3S-TC-N		550m
3	HOATECH	HTI8512-X5ATO		550m
4	SPACE SHUTTLE	S56L-S85-6L-N		550m
5	LuminentOIC	SP-GB-LX	Single-mode	10km
		SP-GB-ELX		20km
		SP-GB-XD		50km
6	AVAGO	AFCT-5710PZ		10km
7	APAC	LS38-C3M-TC-N		20km
8	SPACE SHUTTLE	S56L-L13-6L-N		10km

APPENDIX C

X-View

Appendix C X-View

Based on the same function structure of the web management interface (Web UI), X-View is a friendly and ease-of-use windows based utility which is designed to manage multiple devices in an easy operating environment with more color graphic pictures, diagrams, and consistent menus. The following descriptions and pictures will guide you to be familiar with this convenient utility.

Firstly, the operating window will show up when the utility is launched.

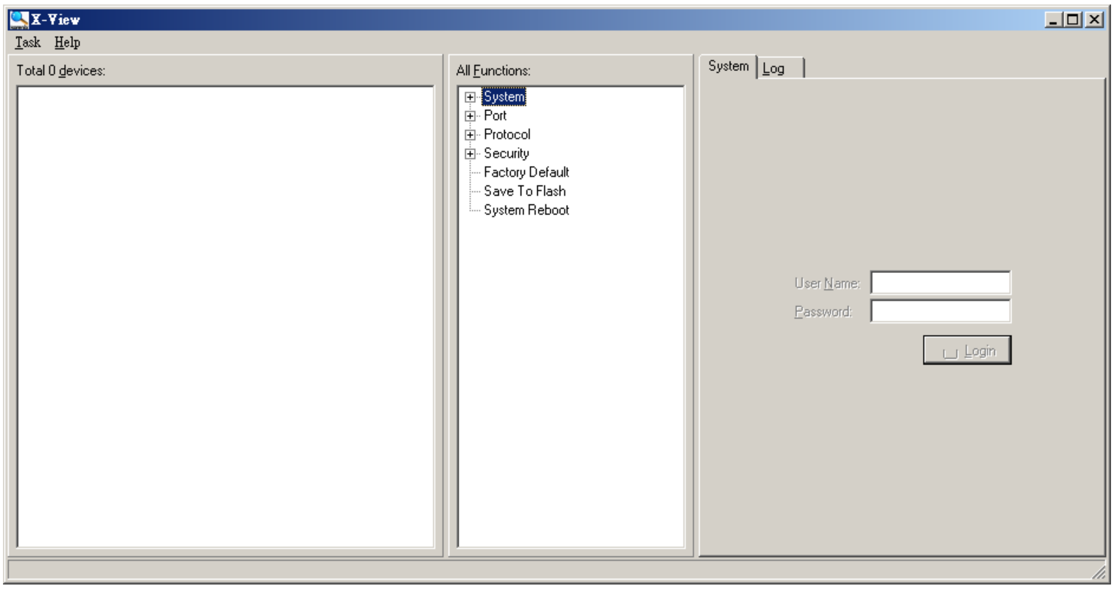


Figure C.1: X-View interface

Move the mouse pointer to the top menu bar, and click on 'Task'. After clicking on 'Task' in the top menu bar, a pull-down menu shows up which including: **D**iscovery, Discovery **F**ilter, **L**ogin, **R**eboot, **R**efresh, Refresh All and E**x**it items.

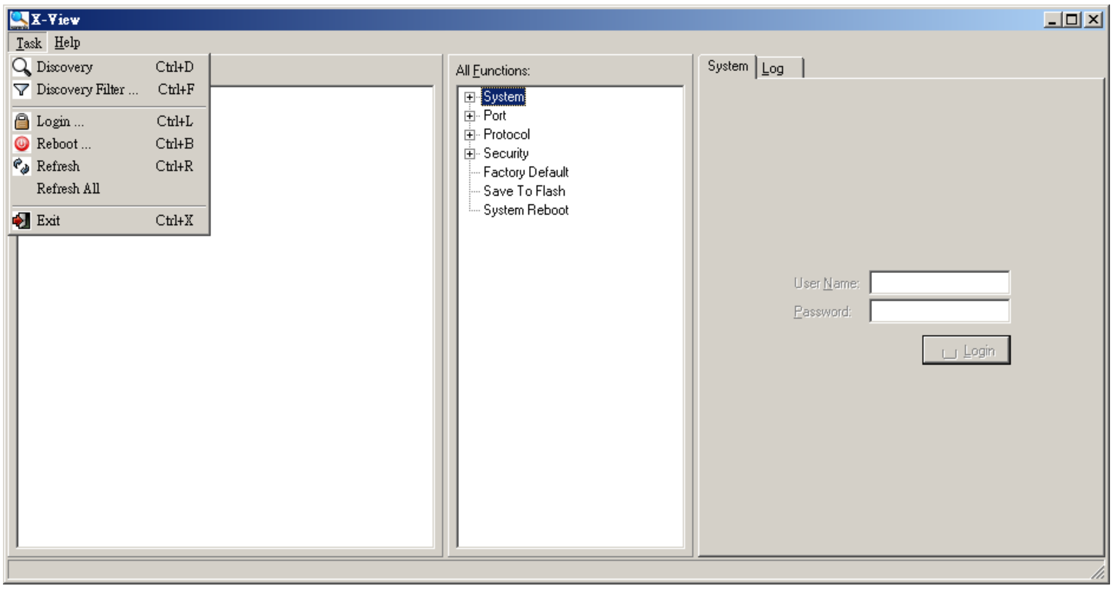
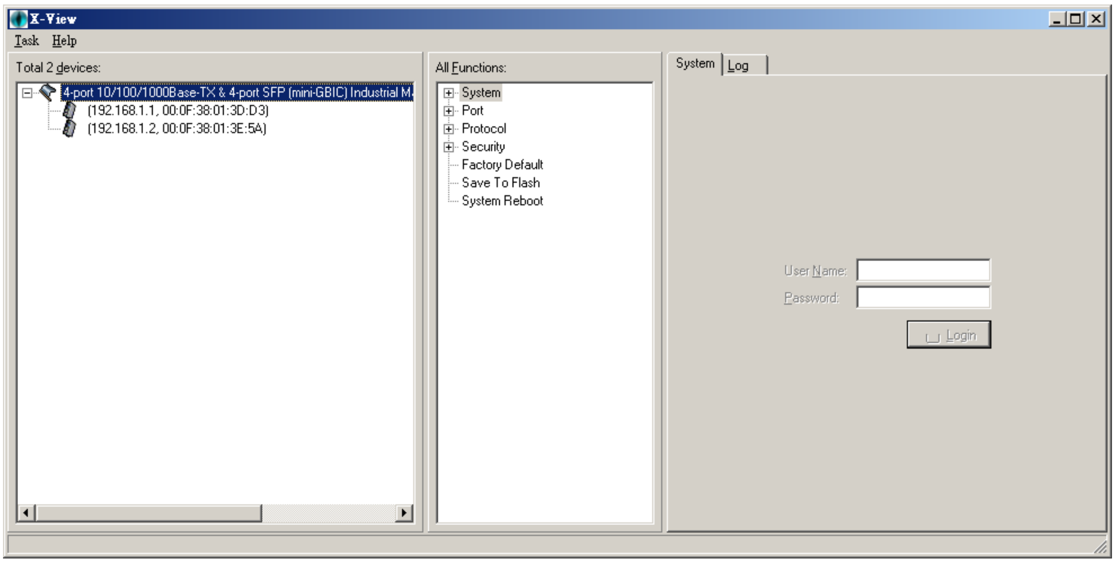


Figure C.2: Items to the 'Task' menu bar

- **Discovery:** Click the mouse point on '**Discovery**' item or press 'Ctrl+D' to search the managed devices on your LAN. Here is an example screenshot:



Total 2 devices:

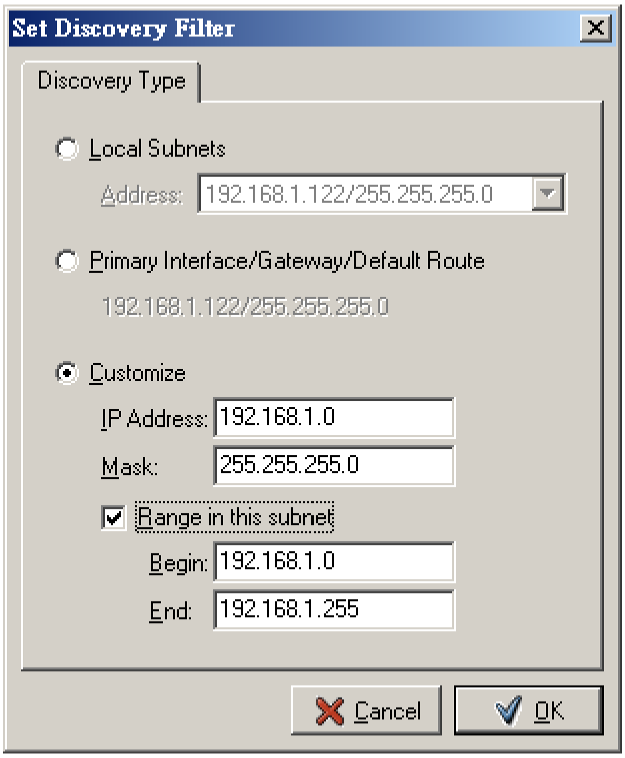
4-port 10/100/1000Base-TX & 4-port SFP (mini-GBIC) Industrial M.

(192.168.1.1, 00:0F:38:01:3D:D3)

(192.168.1.2, 00:0F:38:01:3E:5A)

Figure C.3: Two devices have been discovered

- **Discovery Filter:** Click the mouse pointer on '**Discovery Filter**' item or press 'Ctrl+F' to set the 'Discovery Type'. Here is an example screenshot:



○ Local Subnets

Address: 192.168.1.122/255.255.255.0

○ Primary Interface/Gateway/Default Route

192.168.1.122/255.255.255.0

● Customize

IP Address: 192.168.1.0

Mask: 255.255.255.0

☑ Range in this subnet

Begin: 192.168.1.0

End: 192.168.1.255

Figure C.4: Discovery Filter setting window

There is a radio button group of three selections to set the discovery type. While '**Local Subnets**' radio button is selected and a specified address of local subnet is assigned, which means once you run the function of discovering devices whose IP addresses are in the range of the assigned subnet, will all be detected and shown in the left field. Else if you select the '**Primary Interface/Gateway/Default Route**' radio button, it means you will find the devices whose IP addresses are the same subnet as the primary interface/gateway/default route. Or you can select '**Customize**' radio button to assign an IP address with mask immediately. Besides, you can also mark the check box of

‘**Range in this subnet**’ to assign a range of IP addresses with the begin and the end ones then you will find the devices whose IP addresses are among this range.

- **Login:** Click the mouse pointer on ‘**Login**’ in the top menu bar.

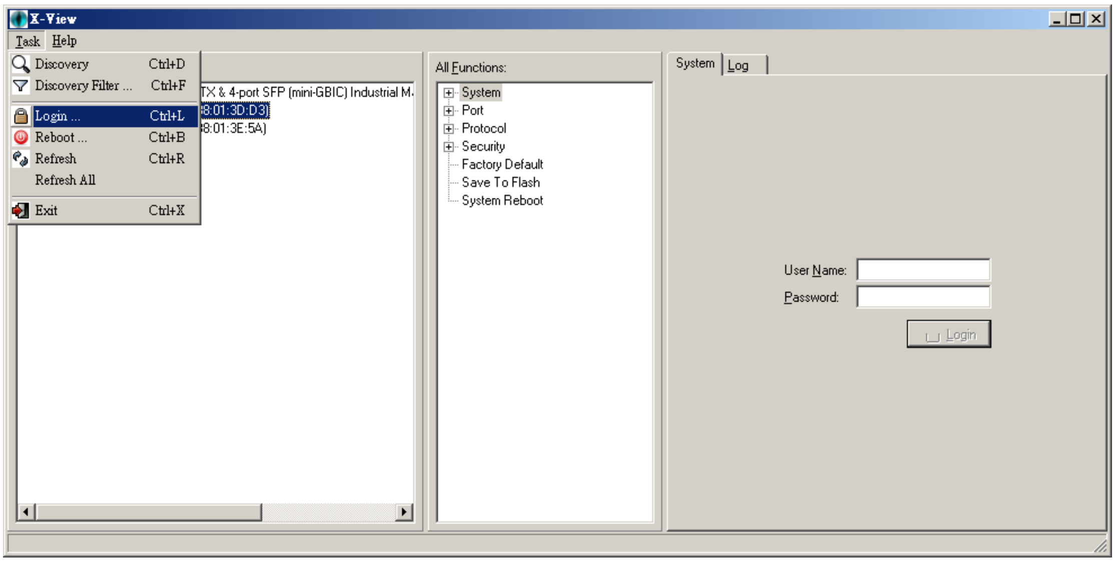
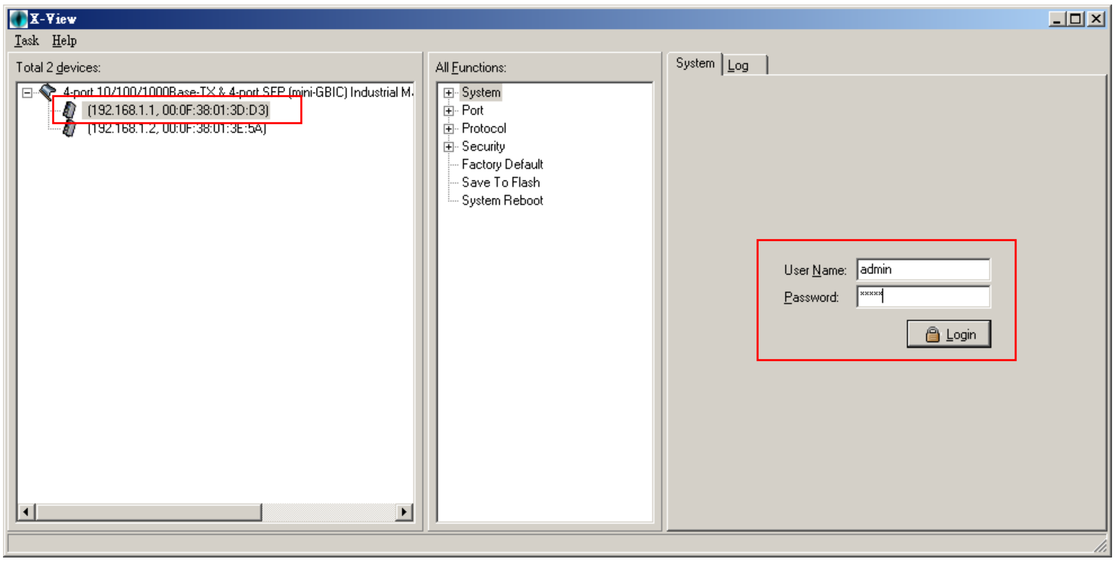


Figure C.5: Login interface

Select any one of the devices in the left tree menu field; the login interface (User Name/Password) on the right side will subsequently be available (see the figure below).



User Name: admin

Password: *****

Figure C.6: User Name/Password interface

- **Reboot:** Click the mouse pointer on ‘**Reboot**’ in the top menu bar.

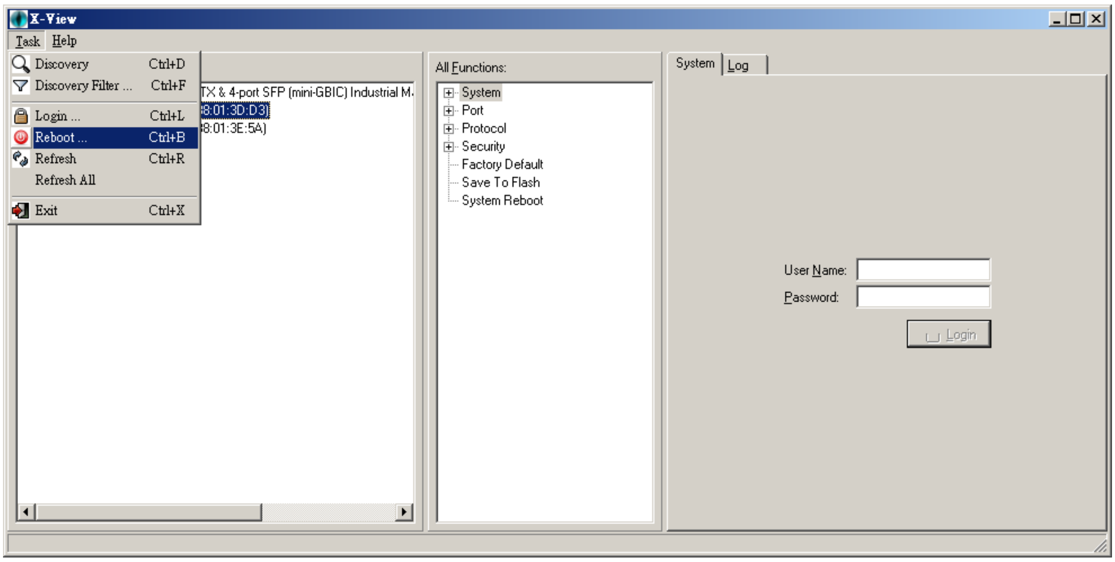


Figure C.7: Reboot function

Select any one of the devices in the left tree menu field; the reboot button on the right side will subsequently be available (see the figure below).

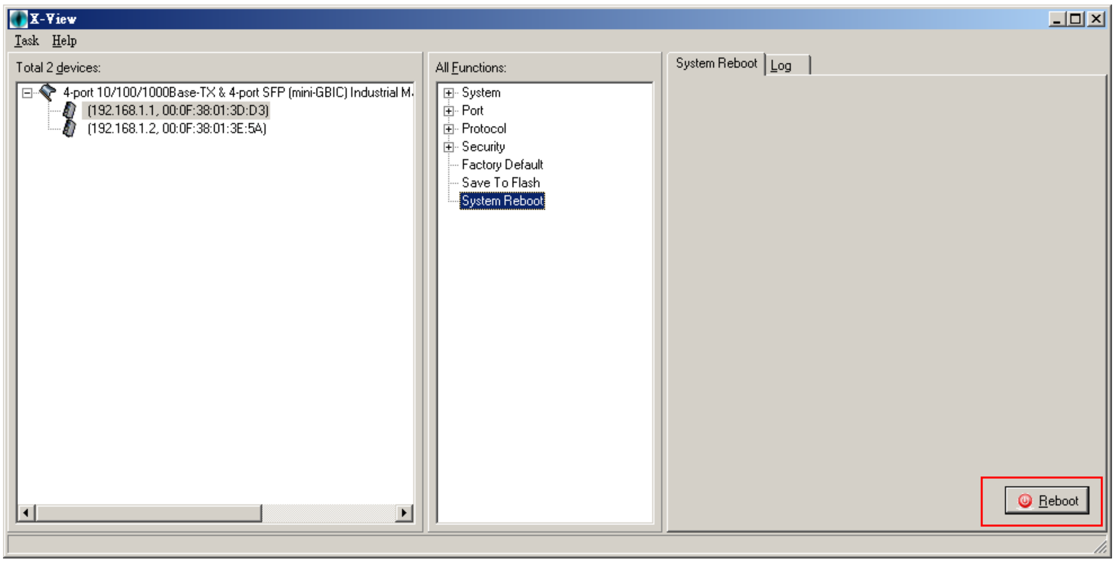
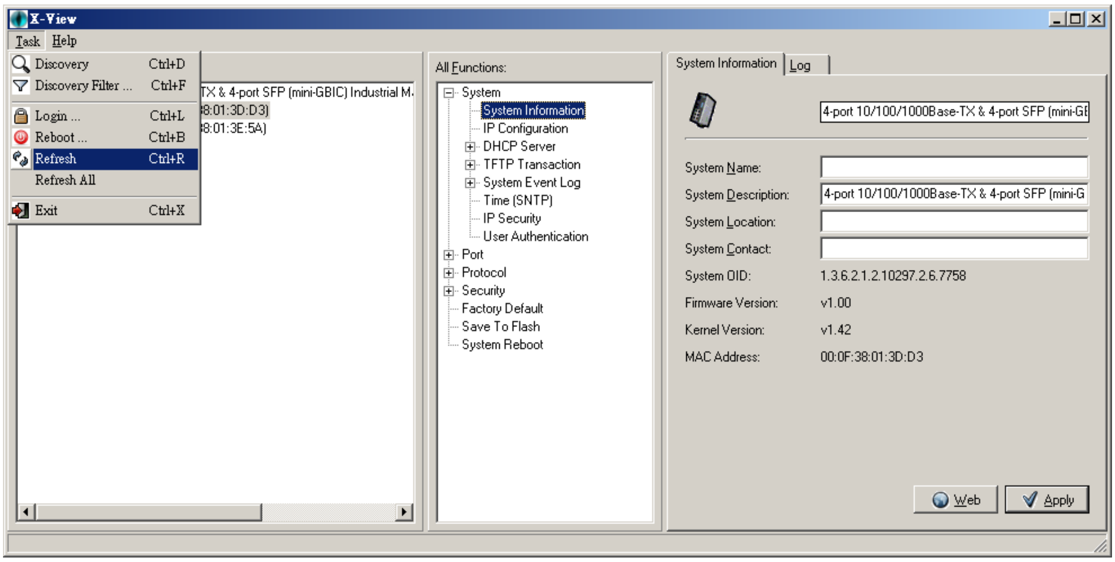


Figure C.8: Press Reboot button to restart the switch

- **Refresh:** Click the mouse pointer on ‘**Refresh**’ in the top menu bar to get the newest information of the current displaying function.



TX & 4-port SFP (mini-GBIC) Industrial M
8:01:3D:D3)
8:01:3E:5A)

4-port 10/100/1000Base-TX & 4-port SFP (mini-GE

System Name:

System Description: 4-port 10/100/1000Base-TX & 4-port SFP (mini-G

System Location:

System Contact:

System OID: 1.3.6.2.1.2.10297.2.6.7758

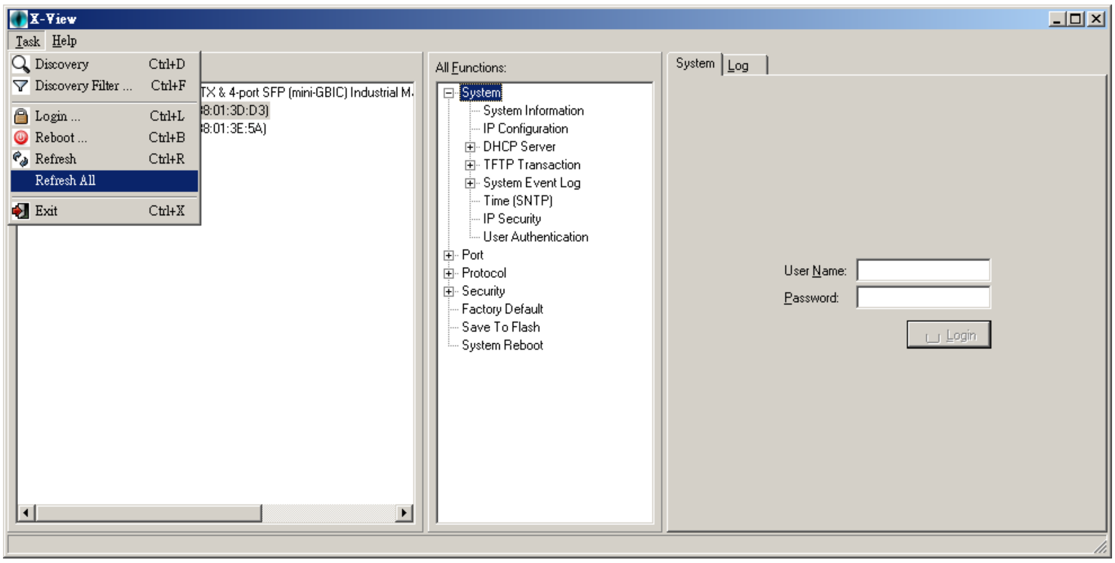
Firmware Version: v1.00

Kernel Version: v1.42

MAC Address: 00:0F:38:01:3D:D3

Figure C.9: Refresh for single function

- **Refresh All:** Click the mouse pointer on '**Refresh All**' in the top menu bar to refresh all the information of the switch.



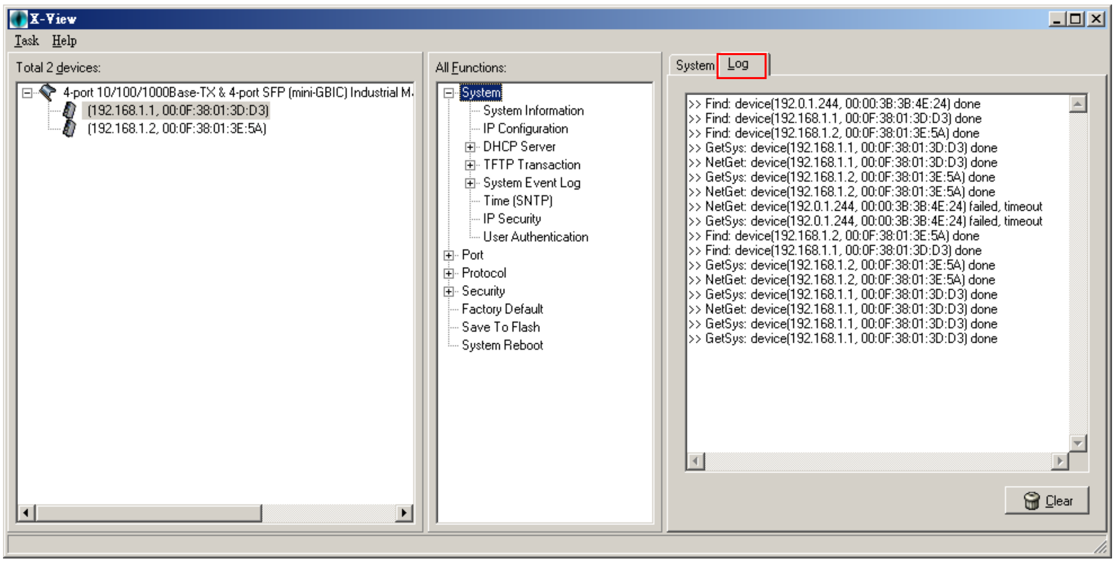
TX & 4-port SFP (mini-GBIC) Industrial M
8:01:3D:D3)
8:01:3E:5A)

User Name:

Password:

Figure C.10: Refresh all the information

You can also make a check of the log by clicking on the ‘Log tab’ on the right side.



```
>> Find: device(192.0.1.244, 00:00:3B:3B:4E:24) done
>> Find: device(192.168.1.1, 00:0F:38:01:3D:D3) done
>> Find: device(192.168.1.2, 00:0F:38:01:3E:5A) done
>> GetSys: device(192.168.1.1, 00:0F:38:01:3D:D3) done
>> NetGet: device(192.168.1.1, 00:0F:38:01:3D:D3) done
>> GetSys: device(192.168.1.2, 00:0F:38:01:3E:5A) done
>> NetGet: device(192.168.1.2, 00:0F:38:01:3E:5A) done
>> NetGet: device(192.0.1.244, 00:00:3B:3B:4E:24) failed, timeout
>> GetSys: device(192.0.1.244, 00:00:3B:3B:4E:24) failed, timeout
>> Find: device(192.168.1.2, 00:0F:38:01:3E:5A) done
>> Find: device(192.168.1.1, 00:0F:38:01:3D:D3) done
>> GetSys: device(192.168.1.2, 00:0F:38:01:3E:5A) done
>> NetGet: device(192.168.1.2, 00:0F:38:01:3E:5A) done
>> GetSys: device(192.168.1.1, 00:0F:38:01:3D:D3) done
>> NetGet: device(192.168.1.1, 00:0F:38:01:3D:D3) done
>> GetSys: device(192.168.1.1, 00:0F:38:01:3D:D3) done
>> GetSys: device(192.168.1.1, 00:0F:38:01:3D:D3) done
```

Figure C.11: Log displaying information

The items in the top menu bar have been introduced. Subsequently, we will go through how to manage the devices via X-View interface.

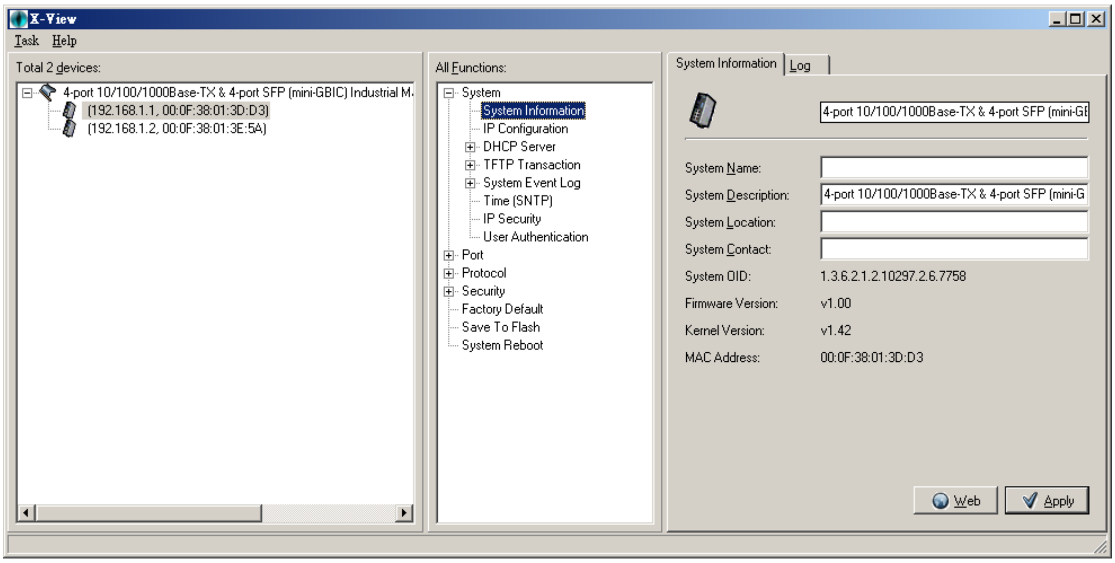
C.1 System

C.1.1 System Information

Assign the system name, location and view the system information

- **System Name**: Assign the name of the switch. The maximum length is 64 bytes.
- **System Description**: Displays the description of switch. Read only cannot be modified.
- **System Location**: Assign the switch physical location. The maximum length is 64 bytes.
- **System Contact**: Enter the name of contact person or organization.
- **System OID**: Displays the strings of numbers of the system OID.
- **Firmware Version**: Displays the switch’s firmware version.
- **Kernel Version**: Displays the kernel software version.
- **MAC Address**: Displays the unique hardware address assigned by manufacturer (default).

Warning *Don’t set “0” for the first segment of the subnet mask and default gateway (000.xxx.xxx.xxx).*
Refresh the web screen if the web could not be displayed while you change the setting.



System Name:
System Description: 4-port 10/100/1000Base-TX & 4-port SFP (mini-G
System Location:
System Contact:
System OID: 1.3.6.2.1.2.10297.2.6.7758
Firmware Version: v1.00
Kernel Version: v1.42
MAC Address: 00:0F:38:01:3D:D3

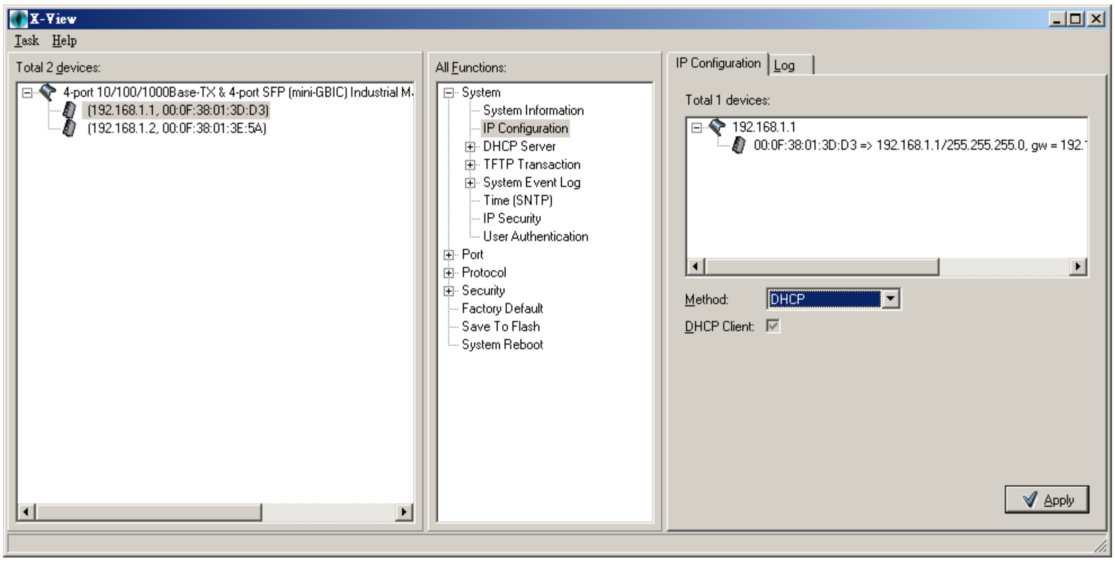
Figure C.12: System information

C.1.2 IP Configuration

User can configure the IP Settings and DHCP client function here.

- **DHCP Client**: Pull down the **Method** select menu item and select the DHCP option to enable the DHCP client function. When DHCP client function is enabled, the industrial switch will be assigned an IP address from the network DHCP server. The default IP address will be replaced by the assigned IP address from DHCP server.

After user click “Apply” button, a popup dialog shows up to ask user entering user name and password.



Total 2 devices:

4-port 10/100/1000Base-TX & 4-port SFP (mini-GBIC) Industrial M.
(192.168.1.1, 00:0F:38:01:3D:D3)
(192.168.1.2, 00:0F:38:01:3E:5A)

Total 1 devices:

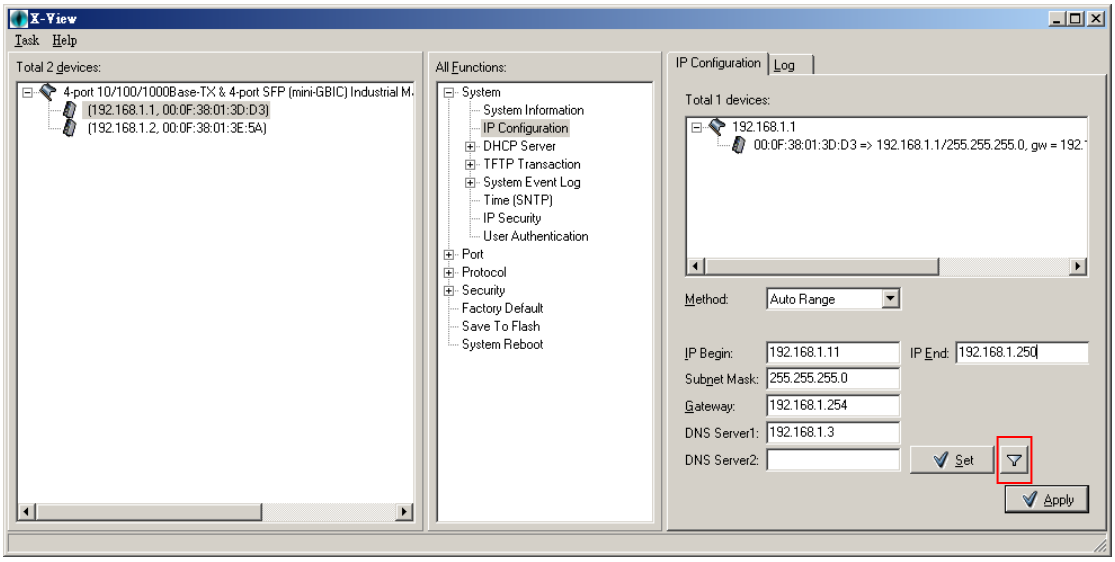
192.168.1.1
00:0F:38:01:3D:D3 => 192.168.1.1/255.255.255.0, gw = 192.1

Method: DHCP

DHCP Client: ☑

Figure C.13: IP Configuration—DHCP

- **Auto Range**: When the **Method** is selected as Auto Range, you can fill in the IP addresses for IP Begin, IP End, Subnet Mask, Gateway, DNS Server1 and DNS Server2 column fields to assign a range of IP addresses. Or you can press the small square button (beside the ‘Set’ button) to load discovery filter as the IP distributing range. Press the ‘Set’ button to carry the setting into effect, and then the device will get an IP address from this assigned range.



Total 2 devices:

4-port 10/100/1000Base-TX & 4-port SFP (mini-GBIC) Industrial M.
(192.168.1.1, 00:0F:38:01:3D:D3)
(192.168.1.2, 00:0F:38:01:3E:5A)

Total 1 devices:

192.168.1.1
00:0F:38:01:3D:D3 => 192.168.1.1/255.255.255.0, gw = 192.1

Method: Auto Range

IP Begin: 192.168.1.11 IP End: 192.168.1.250

Subnet Mask: 255.255.255.0

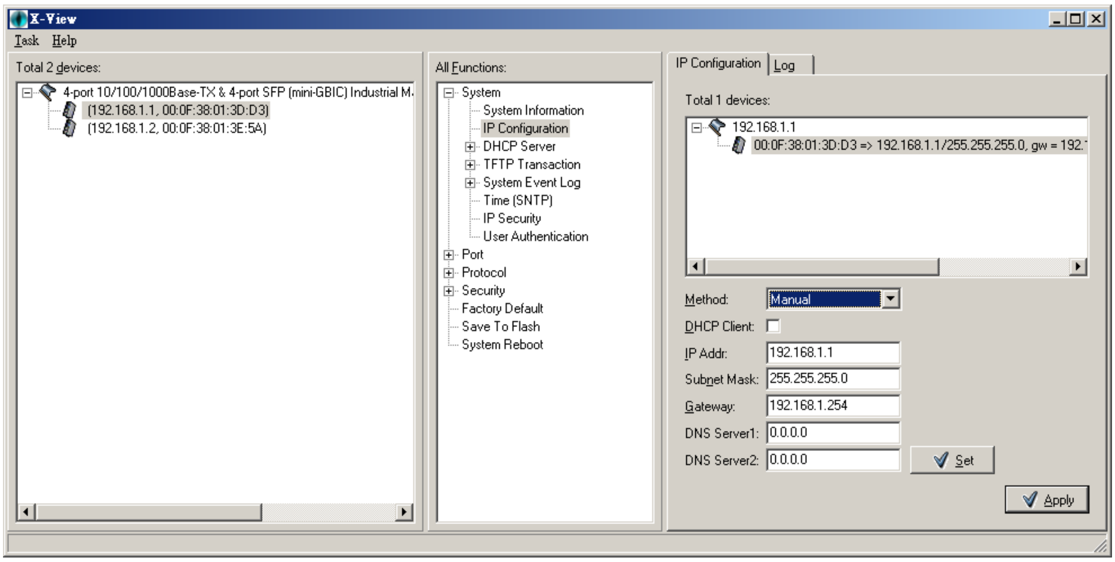
Gateway: 192.168.1.254

DNS Server1: 192.168.1.3

DNS Server2:

Figure C.14: IP Configuration—Auto range

- **Manual**: When the **Method** is selected as Manual, you can enter the IP configuration into the related column fields directly to assign or change the IP configuration. Press the ‘Set’ button to carry the setting into effect.



Total 2 devices:
4-port 10/100/1000Base-TX & 4-port SFP (mini-GBIC) Industrial M
(192.168.1.1, 00:0F:38:01:3D:D3)
(192.168.1.2, 00:0F:38:01:3E:5A)

Total 1 devices:
192.168.1.1
00:0F:38:01:3D:D3 => 192.168.1.1/255.255.255.0, gw = 192.

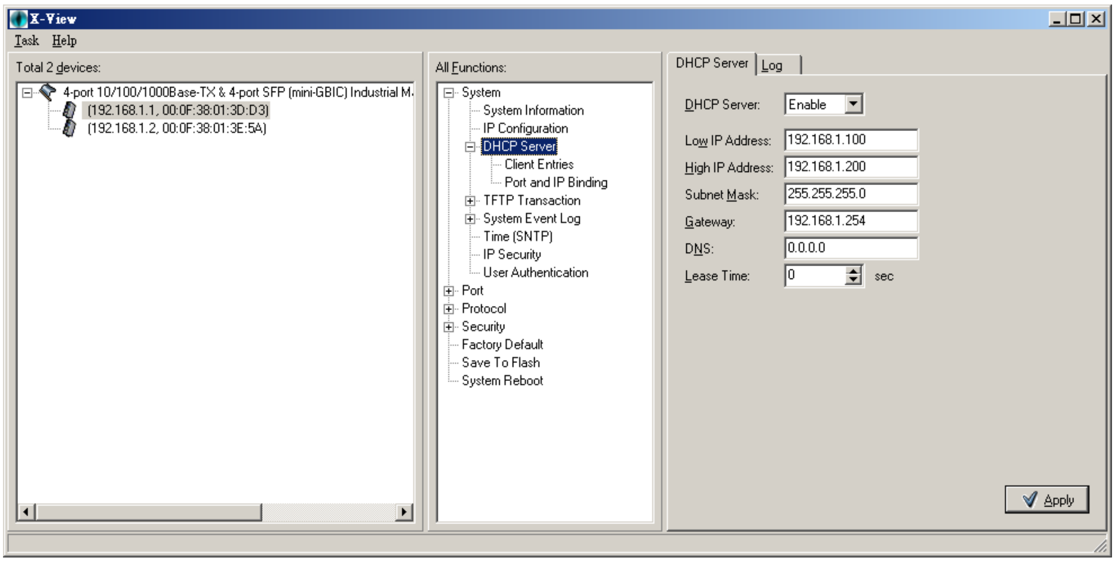
Method: Manual
DHCP Client: □
IP Addr: 192.168.1.1
Subnet Mask: 255.255.255.0
Gateway: 192.168.1.254
DNS Server1: 0.0.0.0
DNS Server2: 0.0.0.0

Figure C.15: IP Configuration—Manual

C.1.3 DHCP Server

The system provides the DHCP server function. Enable the DHCP server function, the switch system will be a DHCP server.

- **DHCP Server:** Enable or Disable the DHCP Server function. Enable – the switch will be the DHCP server on your local network.
- **Low IP Address:** the dynamic IP assign range. Low IP address is the beginning of the dynamic IP assigns range. For example: dynamic IP assigning range is from 192.168.1.100 ~ 192.168.1.200. In contrast, 192.168.1.100 is the Low IP address.
- **High IP Address:** the dynamic IP assign range. High IP address is the end of the dynamic IP assigns range. For example: dynamic IP assign range is from 192.168.1.100 ~ 192.168.1.200. In contrast, 192.168.1.200 is the High IP address.
- **Subnet Mask:** the dynamic IP assign range subnet mask.
- **Gateway:** the gateway in your network.
- **DNS:** Domain Name Server IP Address in your network.
- **Lease Time (sec):** It is the time period that system will reset the dynamic IP assignment to ensure the dynamic IP will not been occupied for a long time or the server doesn’t know that the dynamic IP is idle.



DHCP Server: Enable

Low IP Address: 192.168.1.100

High IP Address: 192.168.1.200

Subnet Mask: 255.255.255.0

Gateway: 192.168.1.254

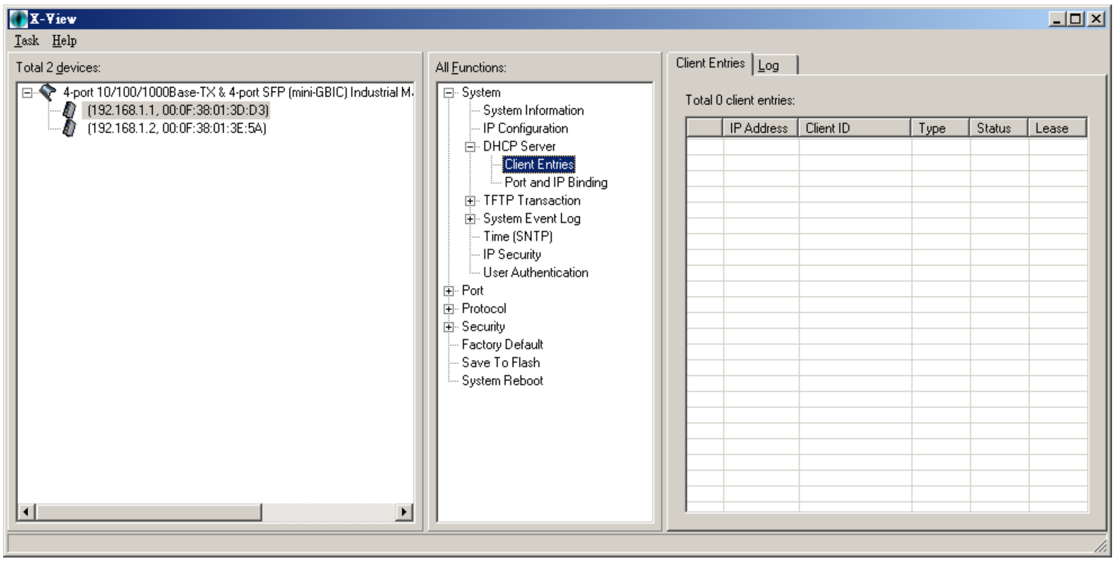
DNS: 0.0.0.0

Lease Time: 0 sec

Figure C.16: DHCP Server interface

Client Entries

When the DHCP server function is active, the system will collect the DHCP client information and displays it here.



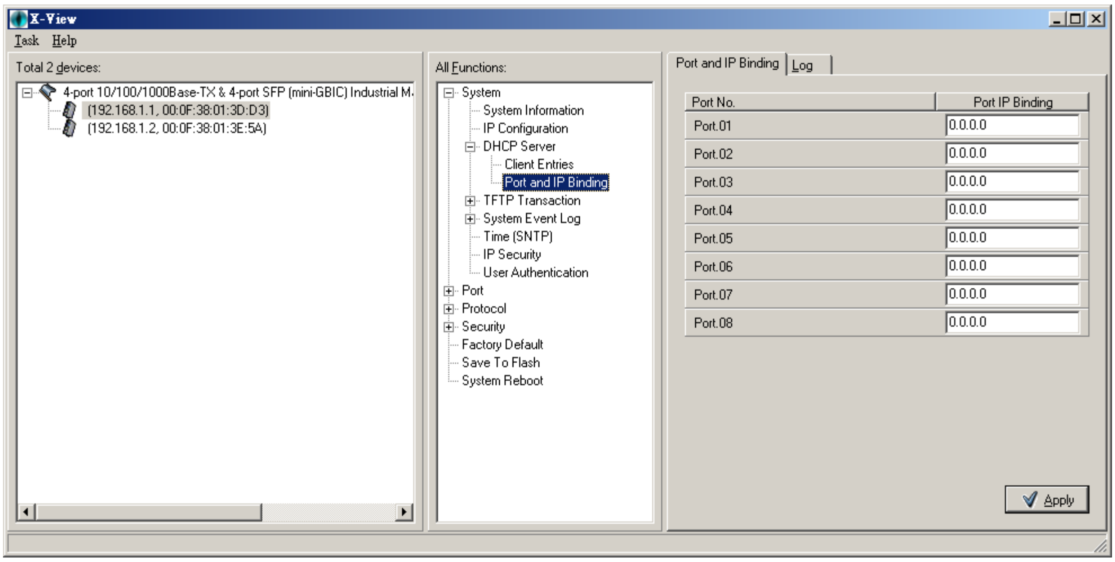
Total 0 client entries:

	IP Address	Client ID	Type	Status	Lease

Figure C.17: DHCP Server – Client Entries

Port and IP Binding

You can assign the specific IP address that is one of the IP addresses in dynamic IP assigning range to the specific port. When the device is connecting to the port and asks for dynamic IP assigning, the system will assign the IP address that has been assigned before to the connected device.



Port No.	Port IP Binding
Port.01	0.0.0.0
Port.02	0.0.0.0
Port.03	0.0.0.0
Port.04	0.0.0.0
Port.05	0.0.0.0
Port.06	0.0.0.0
Port.07	0.0.0.0
Port.08	0.0.0.0

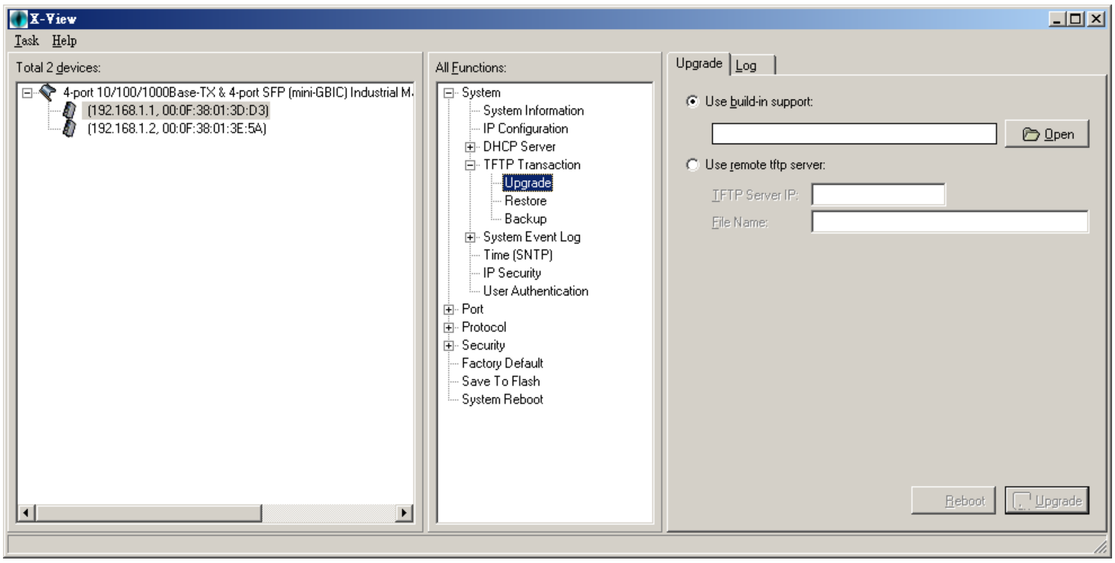
Figure C.18: DHCP Server – Port and IP Binding

C.1.4 TFTP Transaction

Upgrade

It provides two options that allow you to update the switch firmware. Before updating, make sure you have your TFTP server ready and the firmware image is on the TFTP server.

- **Use build-in support:** Click the mouse pointer on the ‘Open’ button to locate file via explorer window.



● Use build-in support:

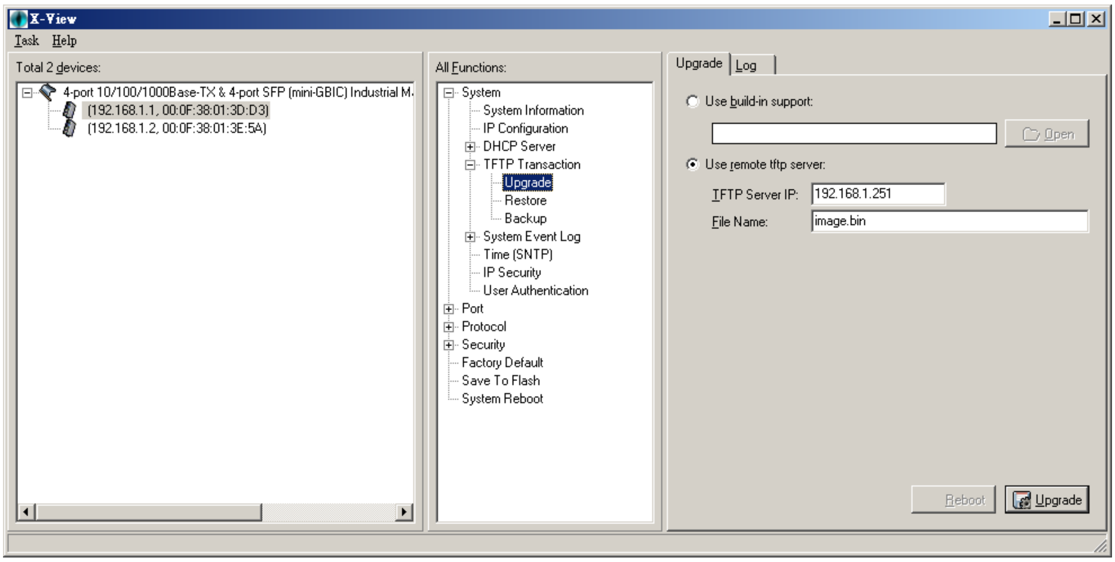
○ Use remote tftp server:

TFTP Server IP:

File Name:

Figure C.19: TFTP Transaction – Upgrade 1

- **Use remote tftp server:** Enter the IP address of the TFTP server and the firmware file name.



○ Use build-in support:

● Use remote tftp server:

TFTP Server IP: 192.168.1.251

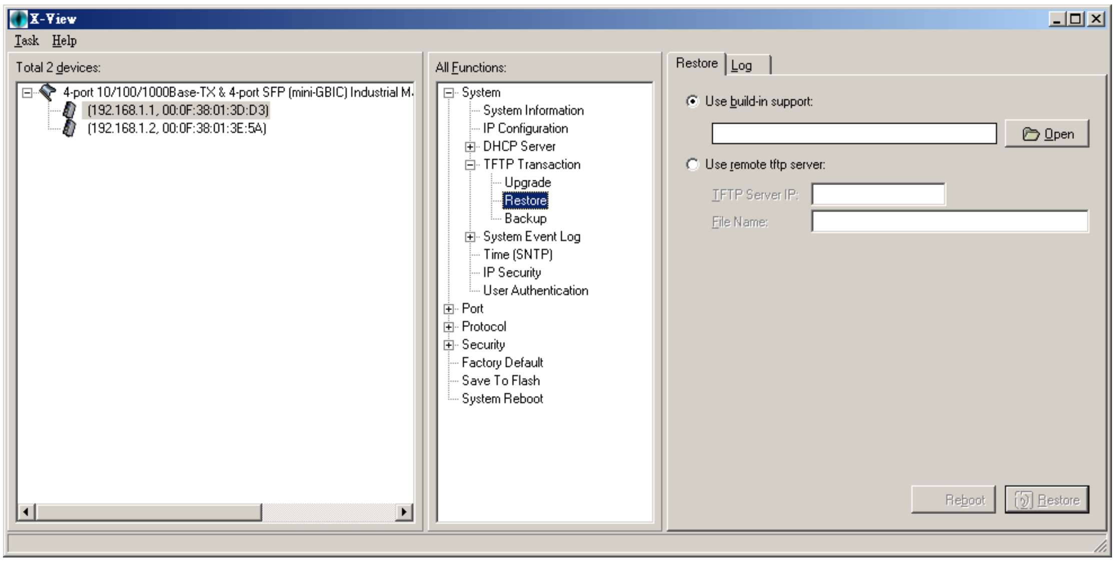
File Name: image.bin

Figure C.20: TFTP Transaction – Upgrade 2

Restore

You can restore Flash ROM value from TFTP server, but you must put the image file on TFTP server first, switch will download back flash image.

- **Use build-in support:** Click the mouse pointer on the 'Open' button to locate file via explorer window.



● Use build-in support:

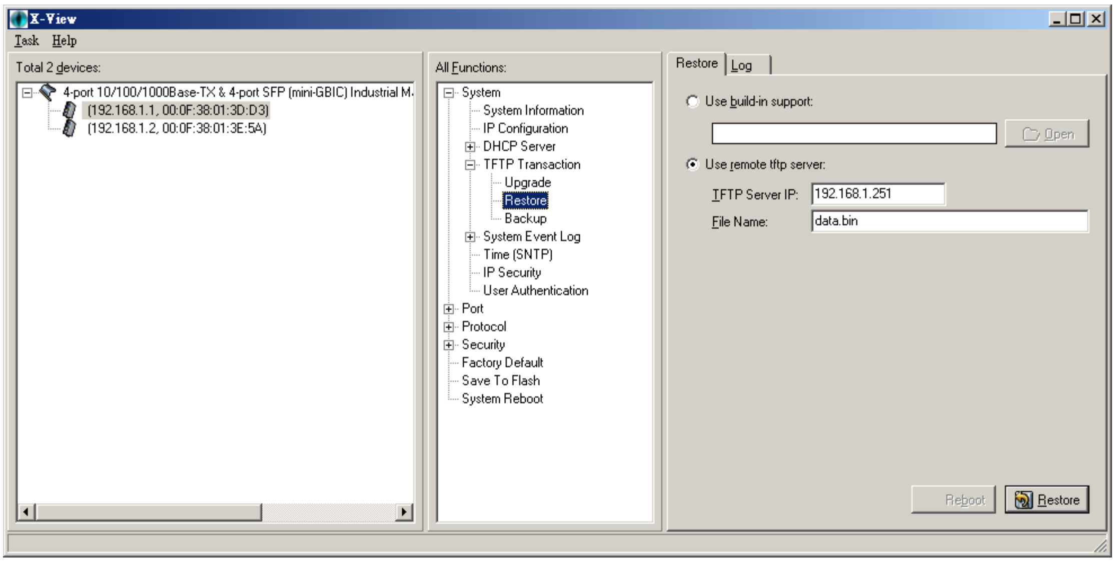
○ Use remote tftp server:

TFTP Server IP:

File Name:

Figure C.21: TFTP Transaction –Restore 1

- **Use remote tftp server:** Enter the IP address of the TFTP server and the firmware file name.



○ Use build-in support:

● Use remote tftp server:

TFTP Server IP: 192.168.1.251

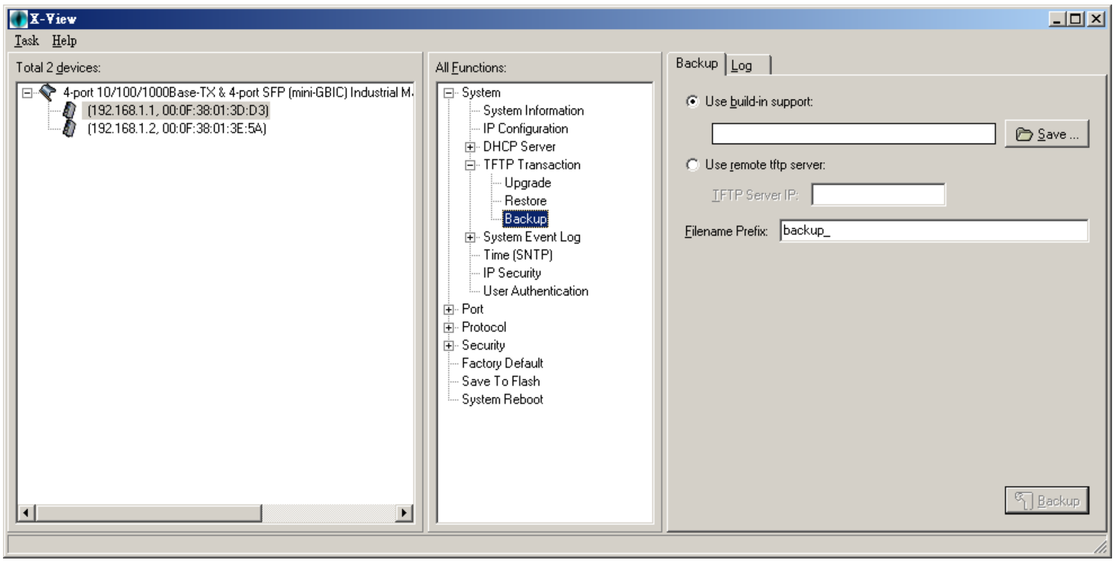
File Name: data.bin

Figure C.22: TFTP Transaction – Restore 2

Backup

You can save current Flash ROM value from the switch to TFTP server that you can go to the TFTP restore configuration page to restore the Flash ROM value later.

- **Use build-in support:** Click the mouse pointer on the 'Save' button to locate a path via explorer window for saving the backup file.



● Use build-in support:

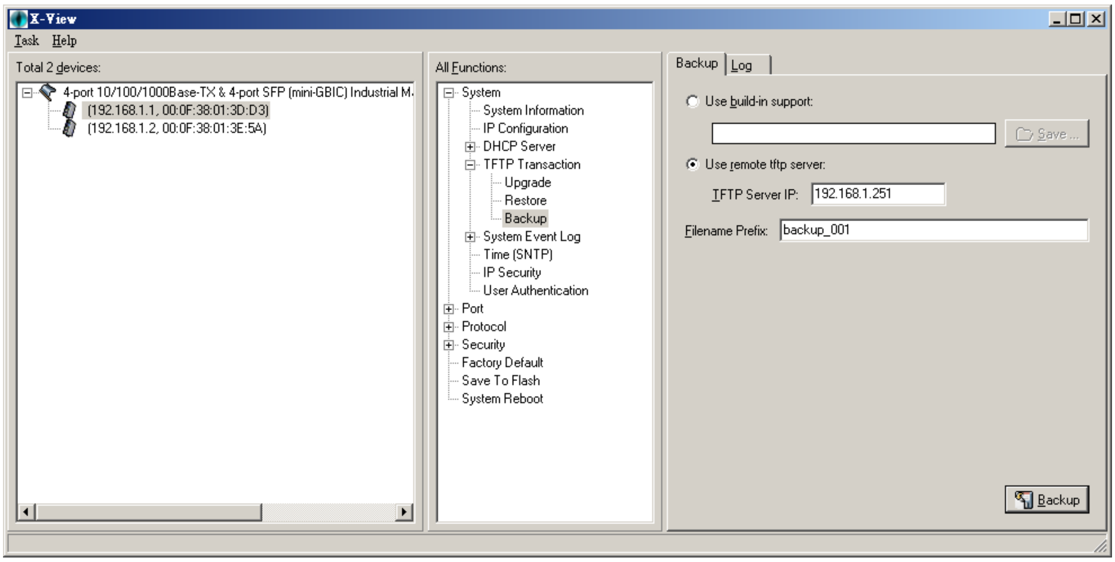
○ Use remote tftp server:

TFTP Server IP:

Filename Prefix: backup_

Figure C.23: TFTP Transaction – Backup 1

- **Use remote tftp server:** Enter the IP address of the TFTP server and the firmware file name.



○ Use build-in support:

● Use remote tftp server:

TFTP Server IP: 192.168.1.251

Filename Prefix: backup_001

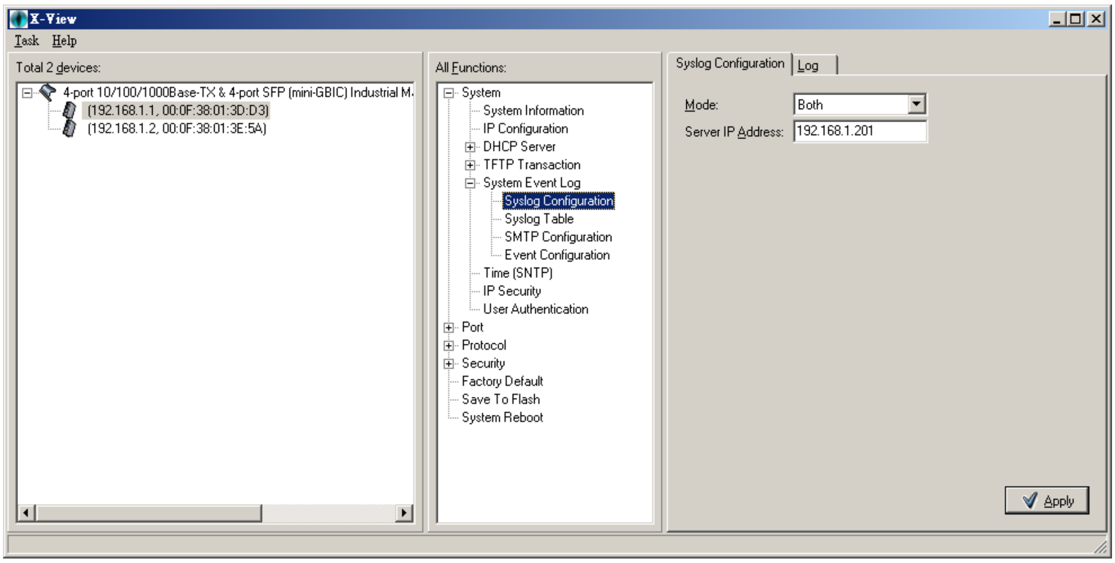
Figure C.24: TFTP Transaction – Backup 2

C.1.5 System Event Log

Syslog Configuration

Configuring the system event mode you want to collect and system log server IP.

- **Mode:** select the system log mode – Client Only, Server Only, or Both.
- **Server IP Address:** assign the system log server IP.



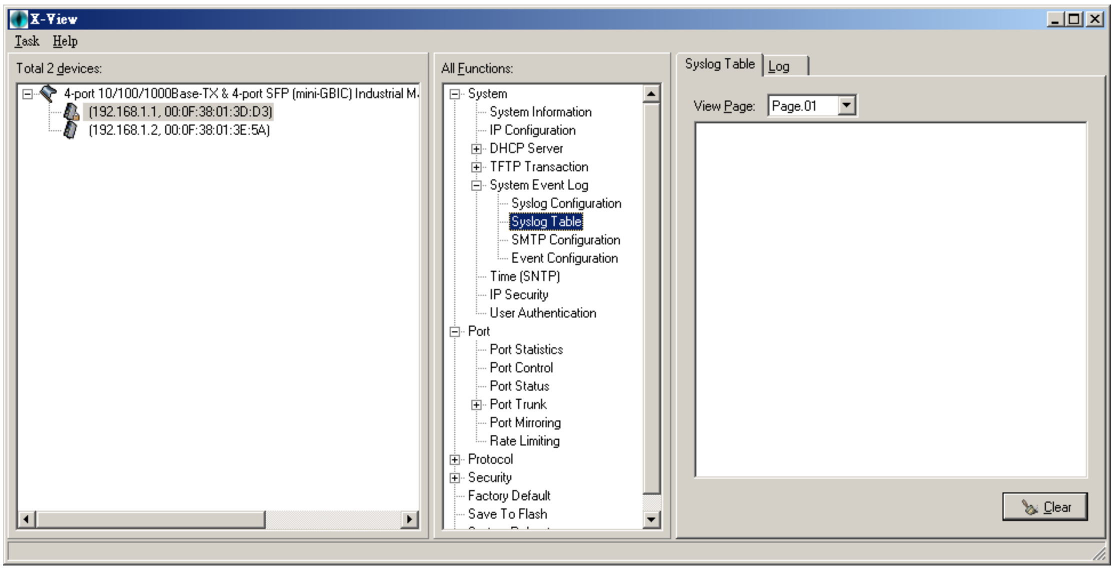
Mode: Both

Server IP Address: 192.168.1.201

Figure C.25: Syslog Configuration

Syslog Table

This function lists the log information.

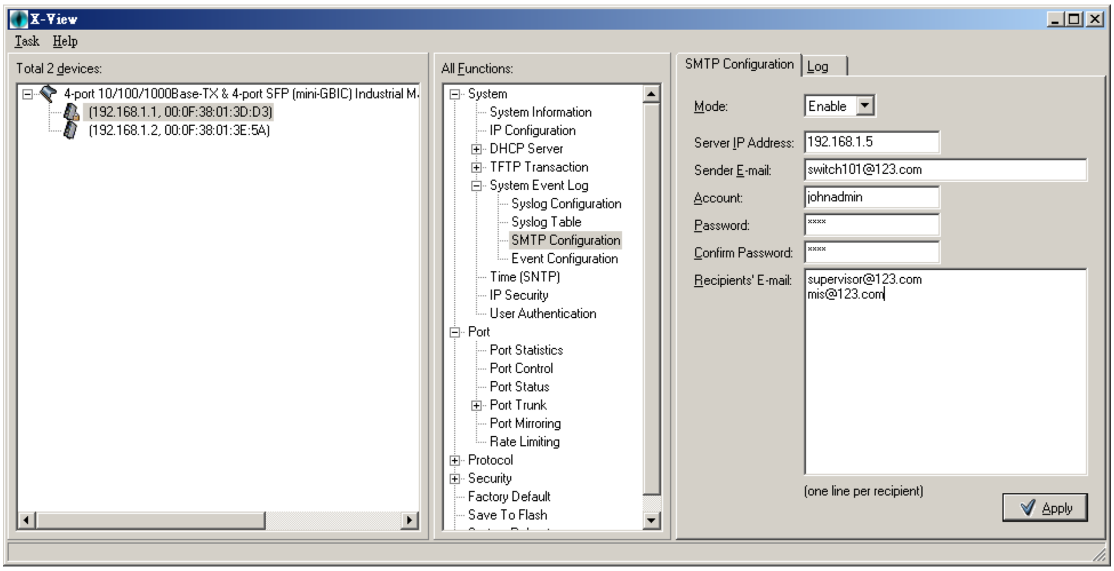


View Page: Page.01

Figure C.26: Syslog Table

SMTP Configuration

You can set up the mail server IP, mail account, account password, and forwarded email account for receiving the event alert.



Mode: Enable

Server IP Address: 192.168.1.5

Sender E-mail: switch101@123.com

Account: johnadmin

Password: ****

Confirm Password: ****

Recipients' E-mail: supervisor@123.com
mis@123.com

(one line per recipient)

Figure C.27: SMTP Configuration

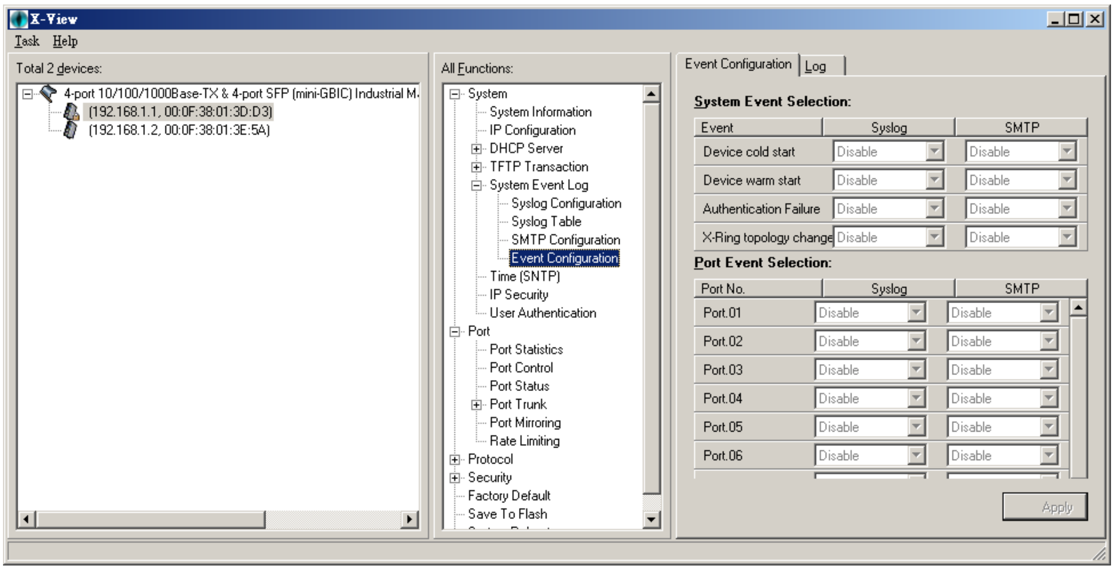
- **Mode:** enable or disable the email alert function.
- **Server IP Address:** set up the mail server IP address (when Mode enabled, this function will then be available).
- **Sender:** key in a complete email address, e.g. switch101@123.com, to identify where the event log comes from.
- **Account:** set up the email account, e.g. johnadmin, to receive the alert. It must be an existing email account on the mail server, which you had set up in SMTP Server IP Address column.
- **Password:** The email account password.
- **Confirm Password:** reconfirm the password.
- **Recipients' E-mail:** you can assign up to 6 e-mail accounts to receive the alert.

Event Configuration

You can select the ‘Syslog’ and ‘SMTP’ events. When selected events occur, the system will send out the log information. Also, per port log and SMTP events can be selected. After configuring, Click ‘Apply’.

- **System Event selection:** 4 selections – Device cold start, Device warm start, SNMP Authentication Failure, and X-ring topology change. Pull down the selection menu items to select the events. When selected events occur, the system will issue the logs.
    - ➢ **Device cold start:** when the device executes cold start action, the system will issue a log event.
    - ➢ **Device warm start:** when the device executes warm start, the system will issue a log event.
    - ➢ **Authentication Failure:** when the SNMP authentication fails, the system will issue a log event.
    - ➢ **X-ring topology change:** when the X-ring topology has changed, the system will issue a log event.

- **Port Event selection:** Pull down the selection menu items to select the Syslog and SMTP events of each port. It has 3 selections – **Link Up**, **Link Down**, and **Link UP & Link Down**. Disable means no event is selected.
    - ➢ **Link UP:** the system will issue a log message when port connection is up only.
    - ➢ **Link Down:** the system will issue a log message when port connection is down only.
    - ➢ **Link UP & Link Down:** the system will issue a log message when port connection is up and down.



System Event Selection:

Event	Syslog	SMTP
Device cold start	Disable	Disable
Device warm start	Disable	Disable
Authentication Failure	Disable	Disable
X-Ring topology change	Disable	Disable

Port Event Selection:

Port No.	Syslog	SMTP
Port.01	Disable	Disable
Port.02	Disable	Disable
Port.03	Disable	Disable
Port.04	Disable	Disable
Port.05	Disable	Disable
Port.06	Disable	Disable

Figure C.28: Event Configuration

C.1.6 Time (SNTP)

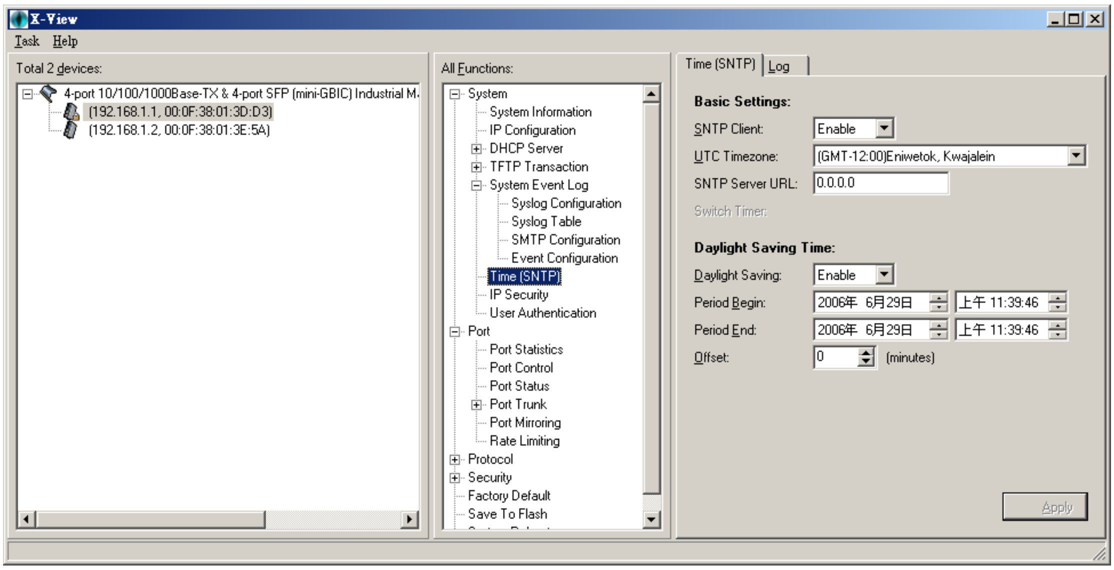
You can configure the SNTP (Simple Network Time Protocol) settings. The SNTP allows you to synchronize switch clocks in the Internet.

Basic Setting:

- **SNTP Client:** enable or disable SNTP function to get the time from the SNTP server.
- **UTC Timezone:** set the switch location time zone. The following table lists the different location time zone for your reference.
- **SNTP Sever URL:** set the SNTP server IP address.

Daylight Saving Time:

- **Daylight Saving:** enable or disable daylight saving time function. When daylight saving time is enabled, you need to configure the daylight saving time period.
- **Period Begin:** set up the Daylight Saving beginning time. It will be different every year.
- **Period End:** set up the Daylight Saving end time. It will be different every year.
- **Offset (mins):** set up the offset time.



Basic Settings:

SNTP Client: Enable

UTC Timezone: (GMT-12:00)Eniwetok, Kwajalein

SNTP Server URL: 0.0.0.0

Switch Timer:

Daylight Saving Time:

Daylight Saving: Enable

Period Begin: 2006年 6月29日 上午 11:39:46

Period End: 2006年 6月29日 上午 11:39:46

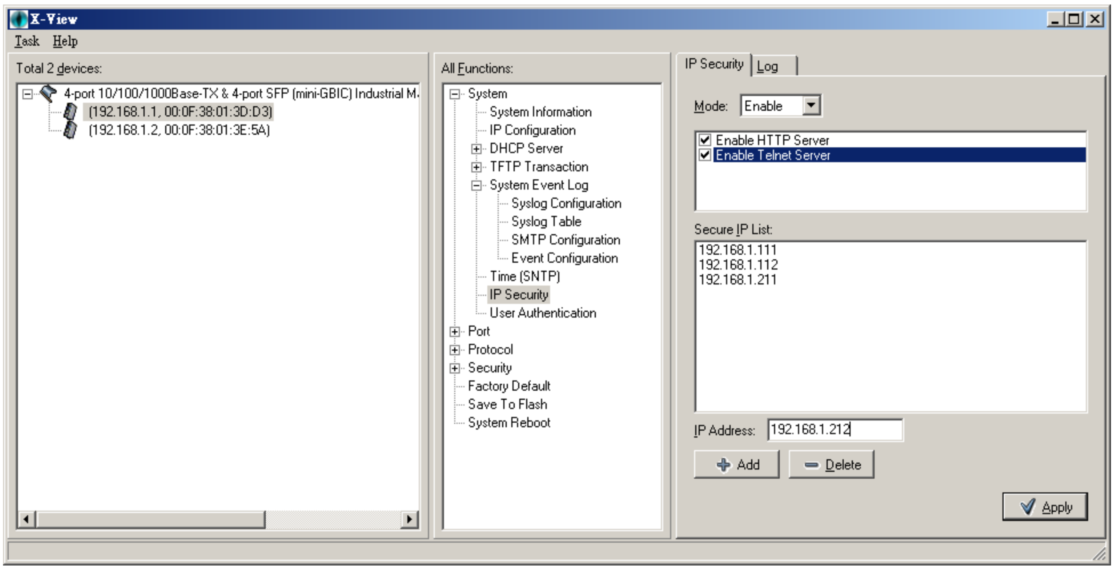
Offset: 0 (minutes)

Figure C.29: Event Configuration

C.1.7 IP Security

IP security function allows user to assign 10 specific IP addresses that have permission to access the switch through the web browser for the securing switch management.

- **Mode:** when this option is in Enable mode, the 'Enable HTTP Server' and 'Enable Telnet Server' check boxes will then be available.
- **Enable HTTP Server:** when this check box is marked, the IP addresses among Security IP1 ~ IP10 will be allowed to access via HTTP service.
- **Enable Telnet Server:** when checked, the IP addresses among Security IP1 ~ IP10 will be allowed to access via telnet service.
- **Security IP 1 ~ 10:** Assign up to 10 specific IP address. Only these 10 IP address can access and manage the switch through the Web browser
- And then, click 'Apply' button to apply the configuration.



Mode: Enable

☑ Enable HTTP Server

☑ Enable Telnet Server

Secure IP List:

192.168.1.111
192.168.1.112
192.168.1.211

IP Address: 192.168.1.212

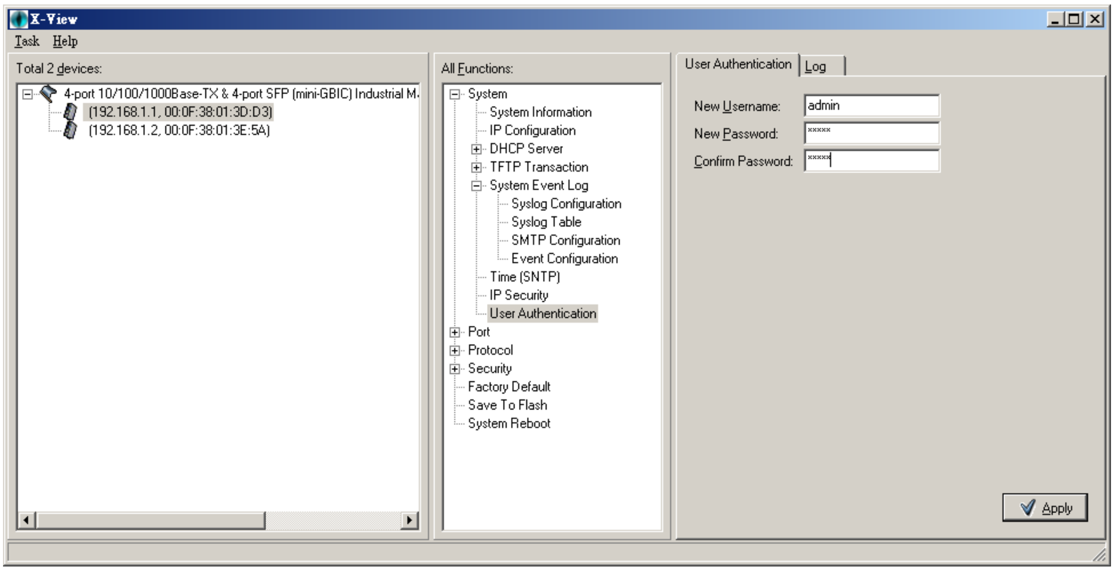
Figure C.30: IP Security

Note *Remember to execute the "Save Configuration" action, otherwise the new configuration will lose when switch power off.*

C.1.8 User Authentication

Change web management login user name and password for the management security issue.

- **User name:** Key in the new user name (The default is "admin")
- **Password:** Key in the new password (The default is "admin")
- **Confirm password:** Re-type the new password
- And then, click 'Apply' button to apply the configuration.



New Username: admin

New Password: *****

Confirm Password: *****

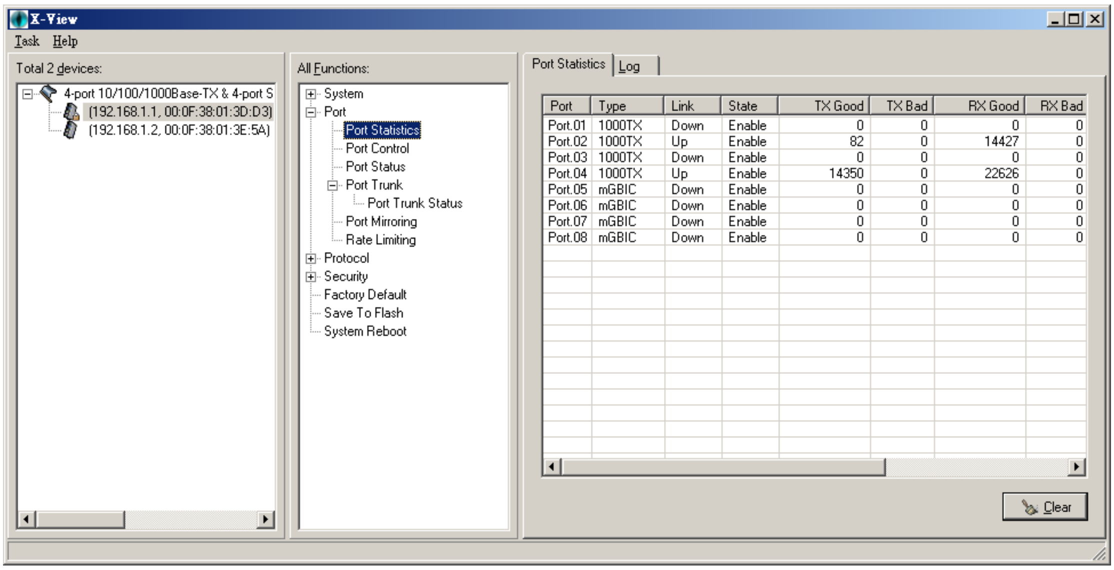
Figure C.31: User Authentication

C.2 Port

C.2.1 Port Statistics

The following information provides the current port statistic information.

- **Port:** The port number.
- **Type:** Displays the current speed of connection to the port.
- **Link:** The status of linking—'Up' or 'Down'.
- **State:** It's set by Port Control. When the state is disabled, the port will not transmit or receive any packet.
- **Tx Good Packet:** The counts of transmitting good packets via this port.
- **Tx Bad Packet:** The counts of transmitting bad packets (including undersize [less than 64 octets], oversize, CRC Align errors, fragments and jabbers packets) via this port.
- **Rx Good Packet:** The counts of receiving good packets via this port.
- **Rx Bad Packet:** The counts of receiving good packets (including undersize [less than 64 octets], oversize, CRC error, fragments and jabbers) via this port.
- **Tx Abort Packet:** The aborted packet while transmitting.
- **Packet Collision:** The counts of collision packet.
- **Packet Dropped:** The counts of dropped packet.
- **Rx Bcast Packet:** The counts of broadcast packet.
- **Rx Mcast Packet:** The counts of multicast packet.
- Click 'Clear button to clear the information.



Port	Type	Link	State	TX Good	TX Bad	RX Good	RX Bad
Port.01	1000TX	Down	Enable	0	0	0	0
Port.02	1000TX	Up	Enable	82	0	14427	0
Port.03	1000TX	Down	Enable	0	0	0	0
Port.04	1000TX	Up	Enable	14350	0	22626	0
Port.05	mGBIC	Down	Enable	0	0	0	0
Port.06	mGBIC	Down	Enable	0	0	0	0
Port.07	mGBIC	Down	Enable	0	0	0	0
Port.08	mGBIC	Down	Enable	0	0	0	0

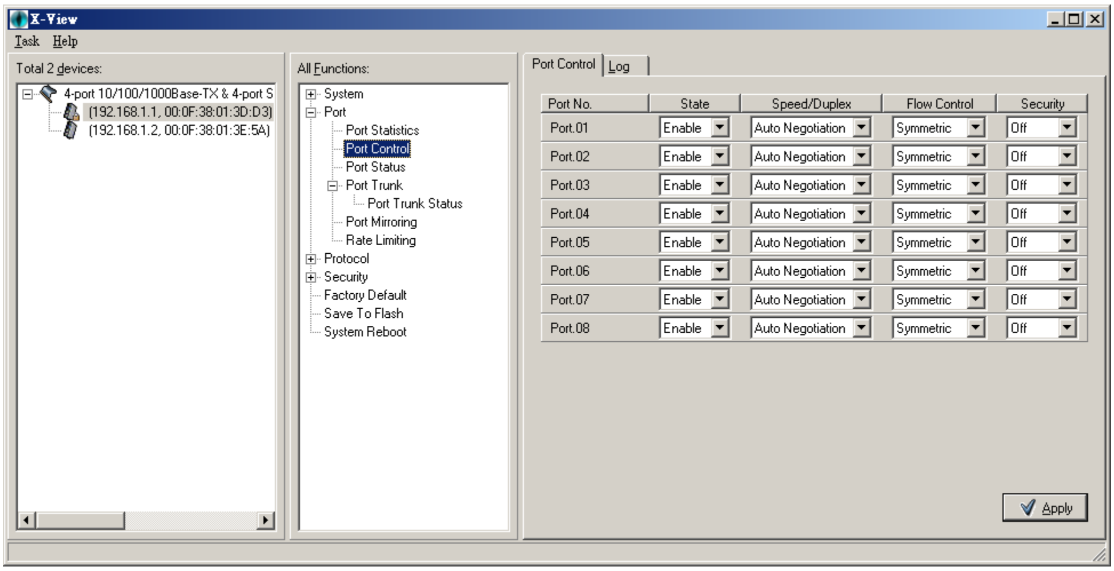
Figure C.32: Port Statistics

C.2.2 Port Control

In Port control, you can view every port status that depends on user setting and the negotiation result.

- **Port No.:** select the port that you want to configure.
- **State:** current port status. The port can be set to disable or enable mode. If the port setting is disable then will not receive or transmit any packet.
- **Speed/Duplex:** set the port link speed.
- **Duplex:** set full-duplex or half-duplex mode of the port.
- **Flow Control:** set flow control function is Symmetric or Asymmetric in Full Duplex mode. The default value is Symmetric.

- **Security:** when its state is “On” that means this port accepts only one MAC address.
- Click ‘Apply’ button to apply the configuration.

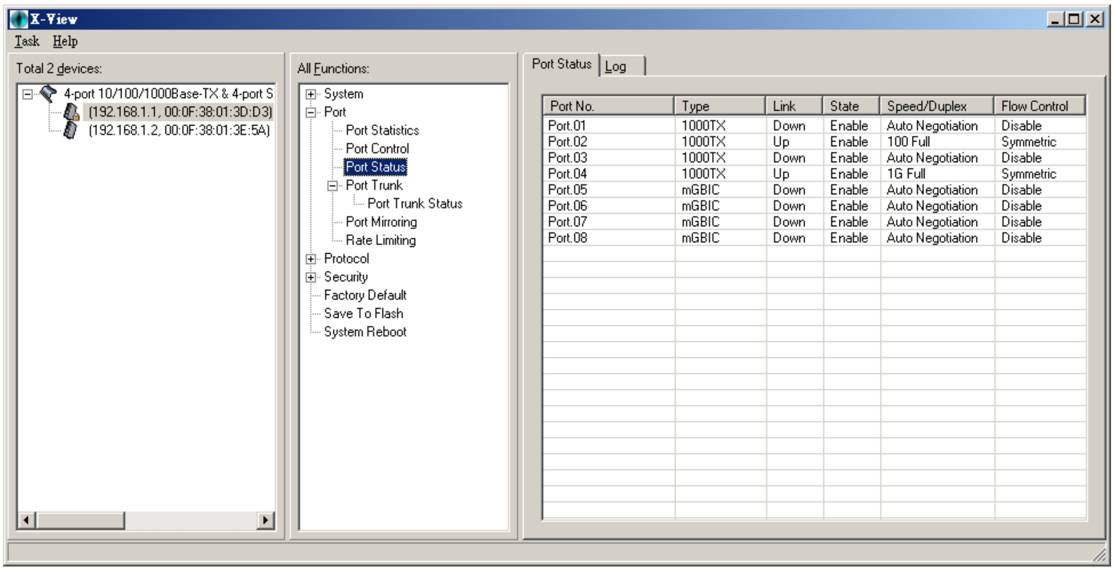


Port No.	State	Speed/Duplex	Flow Control	Security
Port.01	Enable	Auto Negotiation	Symmetric	Off
Port.02	Enable	Auto Negotiation	Symmetric	Off
Port.03	Enable	Auto Negotiation	Symmetric	Off
Port.04	Enable	Auto Negotiation	Symmetric	Off
Port.05	Enable	Auto Negotiation	Symmetric	Off
Port.06	Enable	Auto Negotiation	Symmetric	Off
Port.07	Enable	Auto Negotiation	Symmetric	Off
Port.08	Enable	Auto Negotiation	Symmetric	Off

Figure C.33: Port Control

C.2.3 Port Status

In Port Status, you can view every port status that depends on user setting and the negotiation result.



Port No.	Type	Link	State	Speed/Duplex	Flow Control
Port.01	1000TX	Down	Enable	Auto Negotiation	Disable
Port.02	1000TX	Up	Enable	100 Full	Symmetric
Port.03	1000TX	Down	Enable	Auto Negotiation	Disable
Port.04	1000TX	Up	Enable	1G Full	Symmetric
Port.05	mGBIC	Down	Enable	Auto Negotiation	Disable
Port.06	mGBIC	Down	Enable	Auto Negotiation	Disable
Port.07	mGBIC	Down	Enable	Auto Negotiation	Disable
Port.08	mGBIC	Down	Enable	Auto Negotiation	Disable

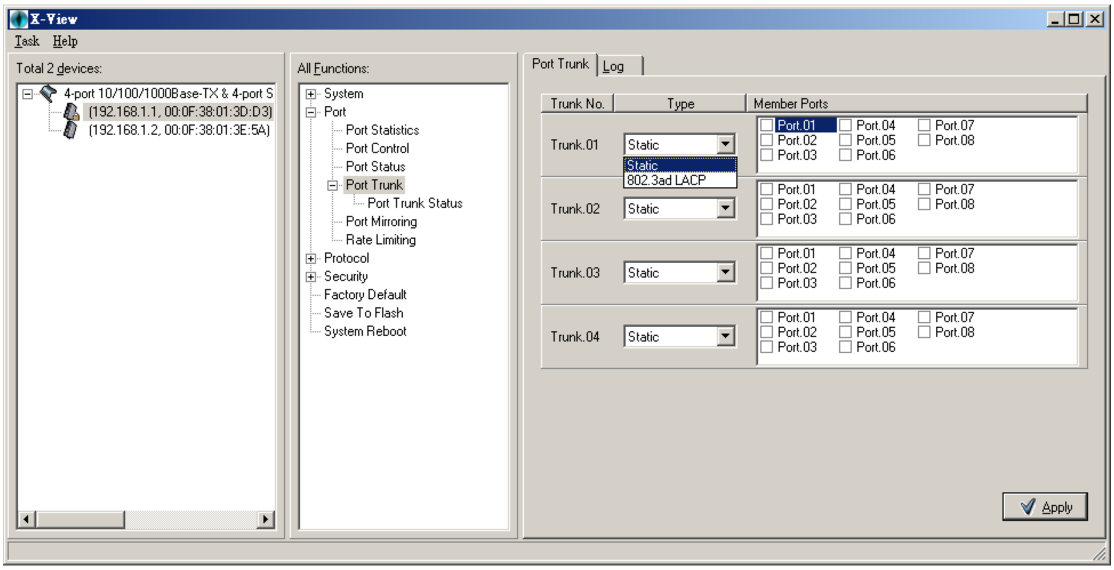
Figure C.34: Port Status

- **Port No.:** select the port that you want to configure.
- **State:** current port status. The port can be set to disable or enable mode. If the port setting is disable then will not receive or transmit any packet.
- **Speed/Duplex:** set the port link speed.
- **Duplex:** set full-duplex or half-duplex mode of the port.
- **Flow Control:** set flow control function is Symmetric or Asymmetric in Full Duplex mode. The default value is Symmetric.
- **Security:** when its state is “On” that means this port accepts only one MAC address.

C.2.4 Port Trunk

The Link Aggregation Control Protocol (LACP) provides a standardized means for exchanging information between Partner Systems on a link to allow their Link Aggregation Control instances to reach agreement on the identity of the Link Aggregation Group to which the link belongs, move the link to that Link Aggregation Group, and enable its transmission and reception functions in an orderly manner. Link aggregation lets you group up to 4 consecutive ports into two dedicated connections. This feature can expand bandwidth to a device on the network. LACP operation requires full-duplex mode, more detail information refers to IEEE 802.3ad.

- **Trunk No.:** There are four trunk groups to provide configuration.
- **Type:** Pull down the selection menu item to select the type as ‘Static’ or ‘802.3ad LACP’.
- **Member ports:** allows max four ports to be aggregated at the same time. With LACP dynamic trunk group, the exceed ports are standby and can be aggregated if work ports fail. If it is static trunk group, the number of ports must be the same as the group member ports.
- Click ’Apply’ button to carry the setting into effect.

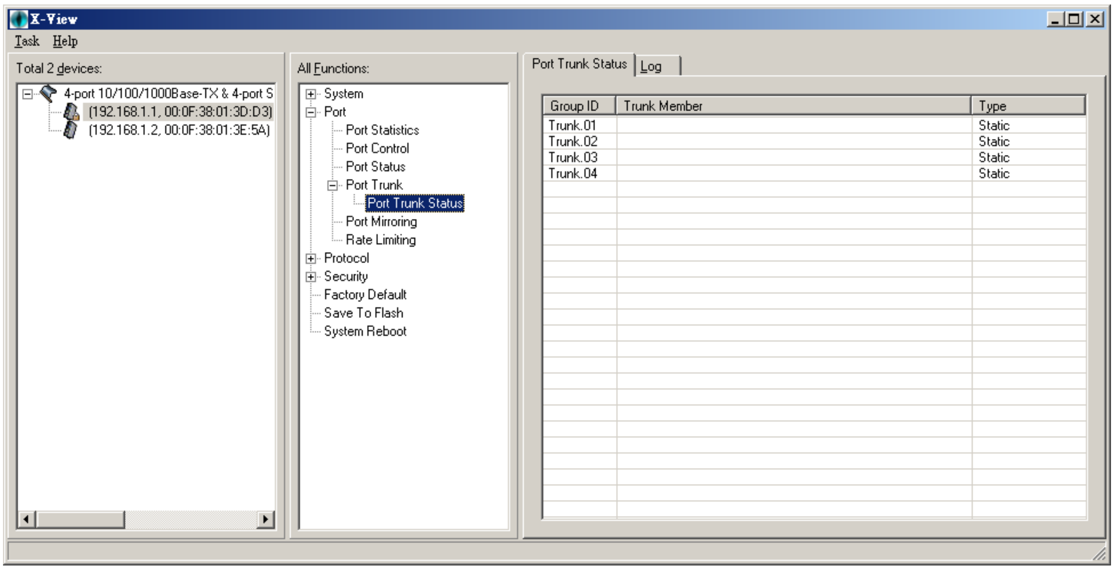


Trunk No.	Type	Member Ports
Trunk.01	Static	□ Port.01 □ Port.02 □ Port.03 □ Port.04 □ Port.05 □ Port.06 □ Port.07 □ Port.08
Trunk.02	Static	□ Port.01 □ Port.02 □ Port.03 □ Port.04 □ Port.05 □ Port.06 □ Port.07 □ Port.08
Trunk.03	Static	□ Port.01 □ Port.02 □ Port.03 □ Port.04 □ Port.05 □ Port.06 □ Port.07 □ Port.08
Trunk.04	Static	□ Port.01 □ Port.02 □ Port.03 □ Port.04 □ Port.05 □ Port.06 □ Port.07 □ Port.08

Figure C.35: Port Trunk

Port Trunk Status:

This function displays the Group ID, Trunk Member and Type.



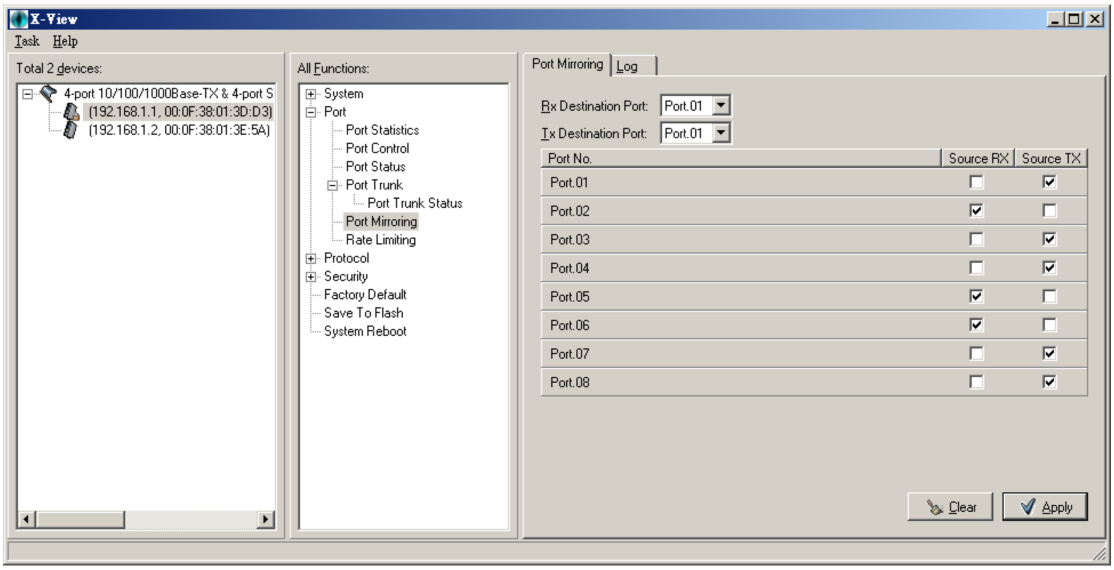
Group ID	Trunk Member	Type
Trunk.01		Static
Trunk.02		Static
Trunk.03		Static
Trunk.04		Static

Figure C.36: Port Trunk Status

C.2.5 Port Mirroring

The Port mirroring is a method for monitor traffic in switched networks. Traffic through ports can be monitored by one specific port. That means traffic goes in or out monitored (source) ports will be duplicated into mirror (destination) port.

- **Rx Destination Port:** There is only one port can be selected to be destination (mirror) port for monitoring RX traffic which come from source port. User can connect mirror port to LAN analyzer or Netxray.
- **Tx Destination Port:** There is only one port can be selected to be destination (mirror) port for monitoring TX traffic which come from source port. User can connect mirror port to LAN analyzer or Netxray.
- Mark the check boxes to monitor source receiving or transmitting packets of each port. And then, click ‘Clear’ button to clear the marks or click ‘Apply’ button to carry the setting into effect.



Rx Destination Port: Port.01

Tx Destination Port: Port.01

Port No.	Source RX	Source TX
Port.01	☐	☑
Port.02	☑	☐
Port.03	☐	☑
Port.04	☐	☑
Port.05	☑	☐
Port.06	☑	☐
Port.07	☐	☑
Port.08	☐	☑

Figure C.37: Port Mirroring

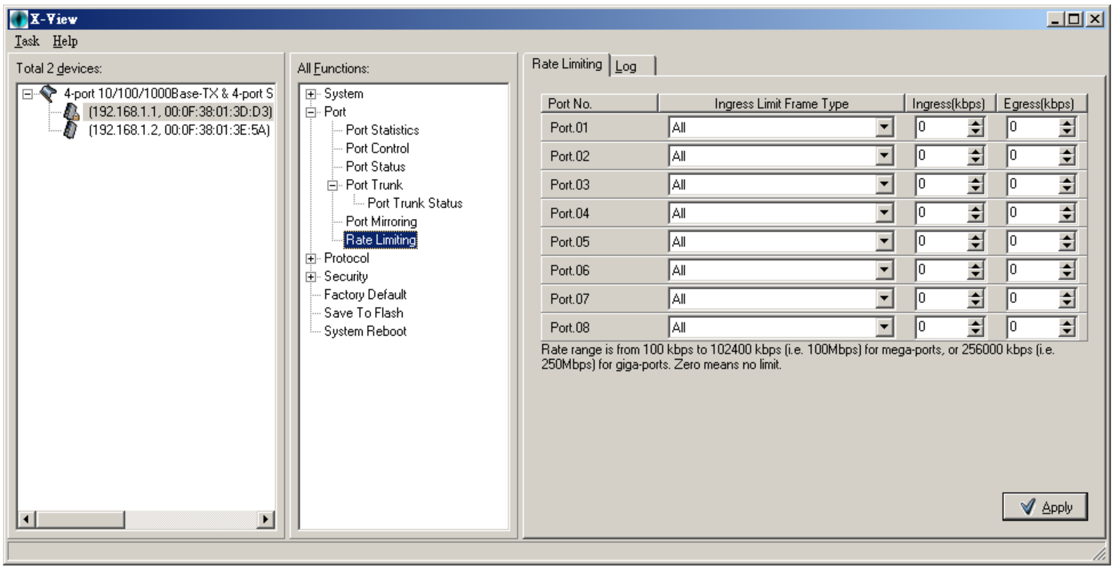
C.2.6 Rate Limiting

Here you can set up every port's bandwidth rate and frame limitation type.

- **Ingress Limit Frame type:** select the frame type that wants to filter. The frame types have 4 options for selecting: All, Broadcast/Multicast/Flooded Unicast, Broadcast/Multicast and Broadcast only. Broadcast/Multicast/Flooded Unicast, Broadcast/Multicast and Bbroadcast only types are only for ingress frames. The egress rate only supports All type.

- All the ports support port ingress and egress rate control. For example, assume port 1 is 10Mbps, users can set it's effective egress rate is 1Mbps, ingress rate is 500Kbps. The switch performs the ingress rate by packet counter to meet the specified rate.

- **Ingress:** Enter the port effective ingress rate (The default value is "8192")
- **Egress:** Enter the port effective egress rate (The default value is "0")
- And then, click 'Apply' to apply the settings.



Port No.	Ingress Limit Frame Type	Ingress(kbps)	Egress(kbps)
Port.01	All	0	0
Port.02	All	0	0
Port.03	All	0	0
Port.04	All	0	0
Port.05	All	0	0
Port.06	All	0	0
Port.07	All	0	0
Port.08	All	0	0

Rate range is from 100 kbps to 102400 kbps (i.e. 100Mbps) for mega-ports, or 256000 kbps (i.e. 250Mbps) for giga-ports. Zero means no limit.

Figure C.38: Rate Limiting

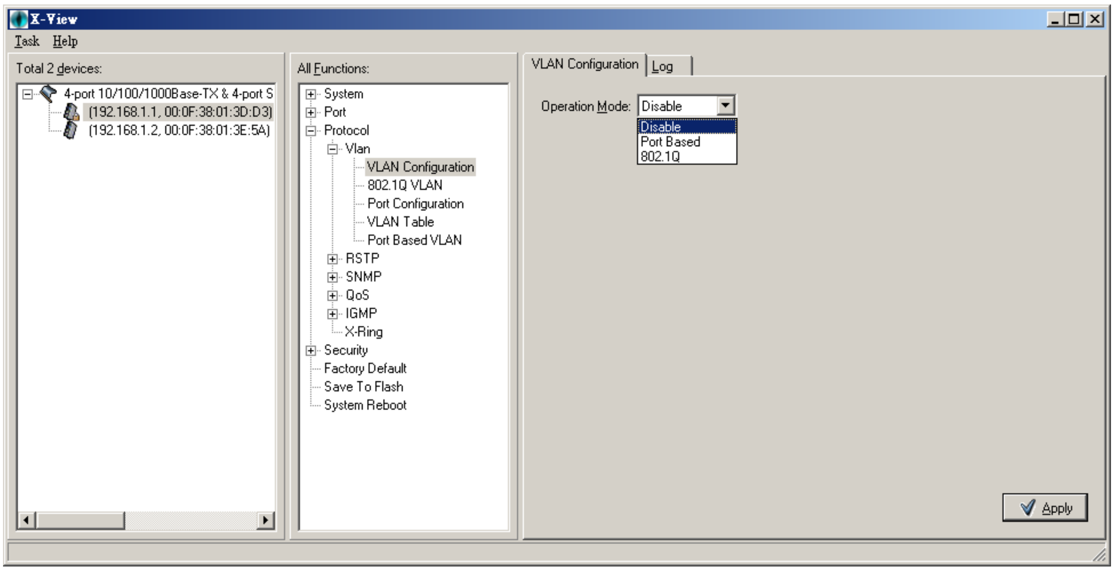
C.3 Protocol

C.3.1 VLAN

VLAN configuration

A Virtual LAN (VLAN) is a logical network grouping that limits the broadcast domain, which would allow you to isolate network traffic, so only the members of the VLAN will receive traffic from the same members of VLAN. Basically, creating a VLAN from a switch is logically equivalent of reconnecting a group of network devices to another Layer 2 switch. However, all the network devices are still plugged into the same switch physically.

The industrial switch supports port-based and 802.1Q (tagged-based) VLAN. The default configuration of VLAN operation mode is “**Disable**”.



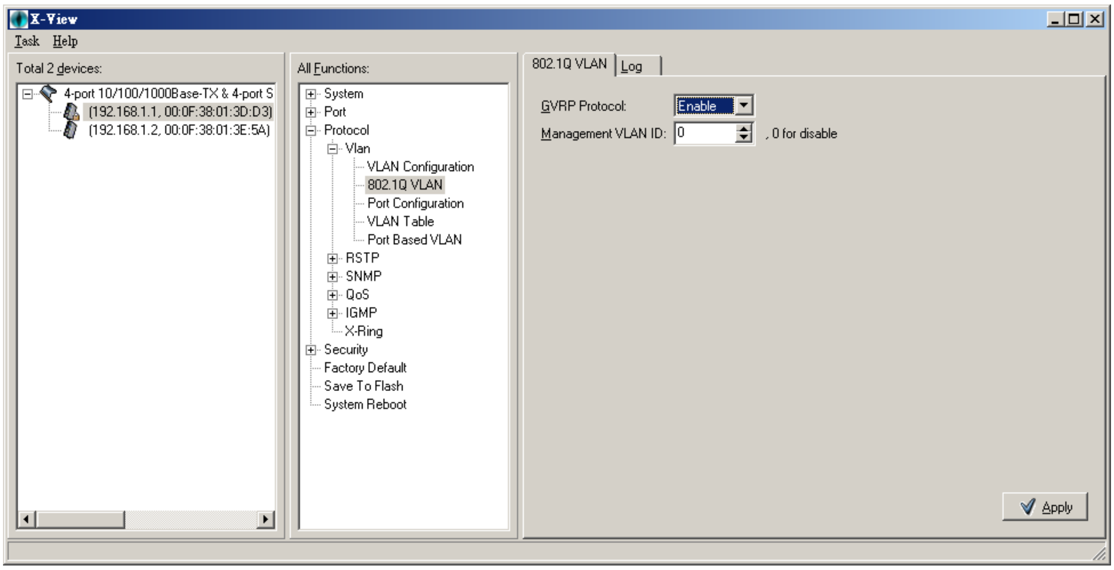
Operation Mode: Disable

Figure C.39: VLAN Configuration

802.1Q VLAN

Tagged-based VLAN is an IEEE 802.1Q specification standard. Therefore, it is possible to create a VLAN across devices from different switch venders. IEEE 802.1Q VLAN uses a technique to insert a “tag” into the Ethernet frames. Tag contains a VLAN Identifier (VID) that indicates the VLAN numbers.
You can create Tag-based VLAN, and enable or disable GVRP protocol. There are 256 VLAN groups to provide configure. Enable 802.1Q VLAN, the all ports on the switch belong to default VLAN, VID is 1. The default VLAN can’t be deleting.

GVRP allows automatic VLAN configuration between the switch and nodes. If the switch is connected to a device with GVRP enabled, you can send a GVRP request using the VID of a VLAN defined on the switch; the switch will automatically add that device to the existing VLAN.



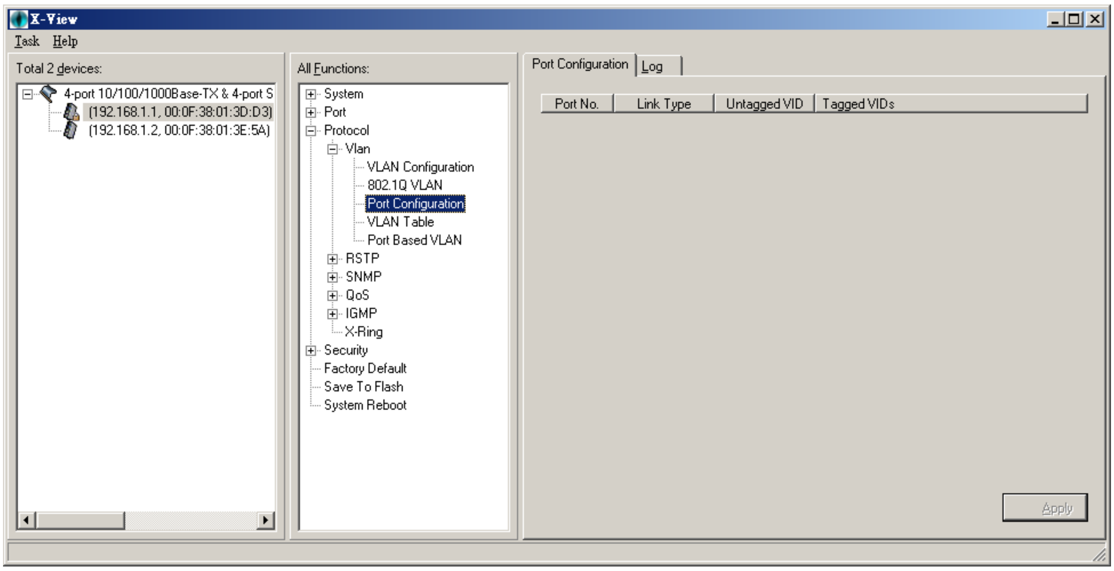
GVRP Protocol: Enable

Management VLAN ID: 0 , 0 for disable

Figure C.40: 802.1Q VLAN

Port Configuration

Set Port No., Link Type, Untagged VID, and Tagged VIDs then click 'Apply' button to apply.



Port No.	Link Type	Untagged VID	Tagged VIDs

Figure C.41: Port Configuration

VLAN Table

This function displays the VLAN table information.

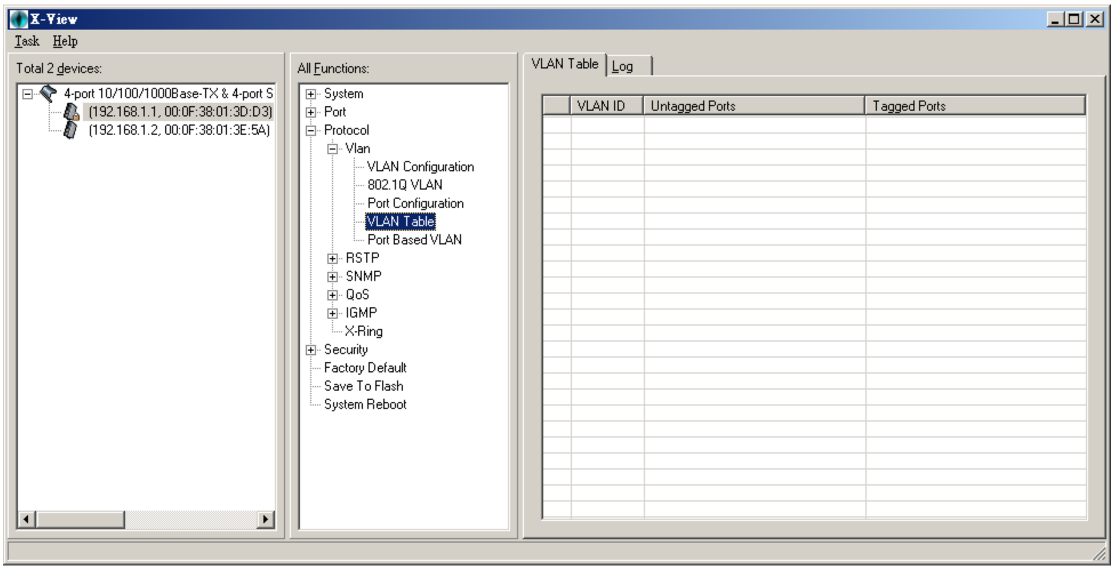


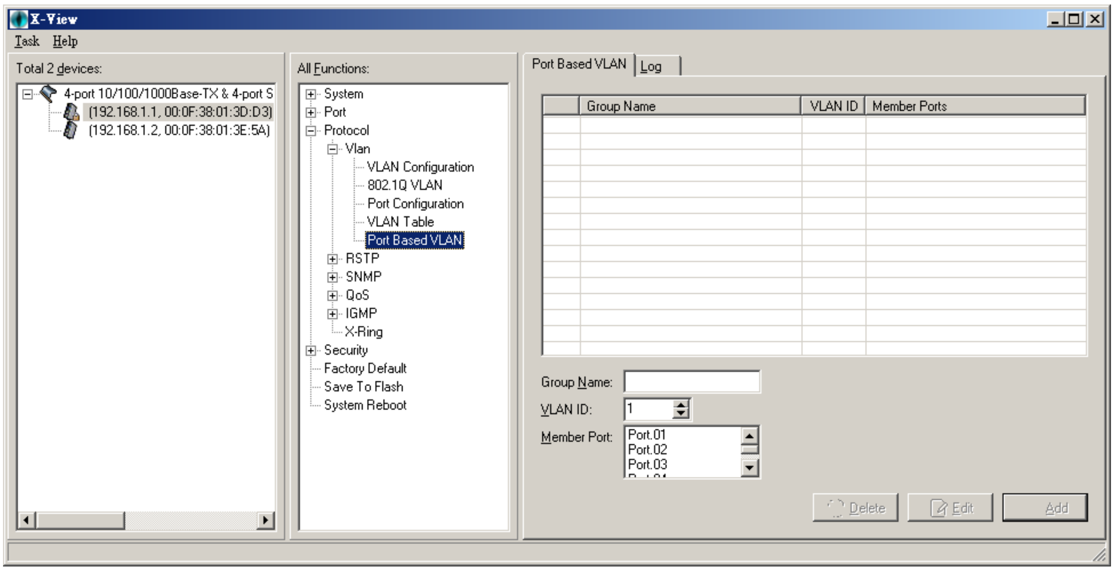
Figure C.42: VLAN Table

Port-based VLAN

Packets can go among only members of the same VLAN group. Note all unselected ports are treated as belonging to another single VLAN. If the port-based VLAN enabled, the VLAN-tagging is ignored.

In order for an end station to send packets to different VLAN groups, it itself has to be either capable of tagging packets it sends with VLAN tags or attached to a VLAN-aware bridge that is capable of classifying and tagging the packet with different VLAN ID based on not only default PVID but also other information about the packet, such as the protocol.

- Click 'Add' button to add a new VLAN group (The maximum VLAN group is up to 64 VLAN groups)
- Entering the VLAN name, group ID and grouping the members of VLAN group



Group Name:

VLAN ID: 1

Member Port: Port.01
Port.02
Port.03

Figure C.43: Port-based VLAN

C.3.2 Rapid Spanning Tree

The Rapid Spanning Tree Protocol (RSTP) is an evolution of the Spanning Tree Protocol and provides for faster spanning tree convergence after a topology change. The system also supports STP and the system will auto detect the connected device that is running STP or RSTP protocol.

- User can view spanning tree information about the Root Bridge.
- User can modify RSTP state. After modification, click 'Apply' button.

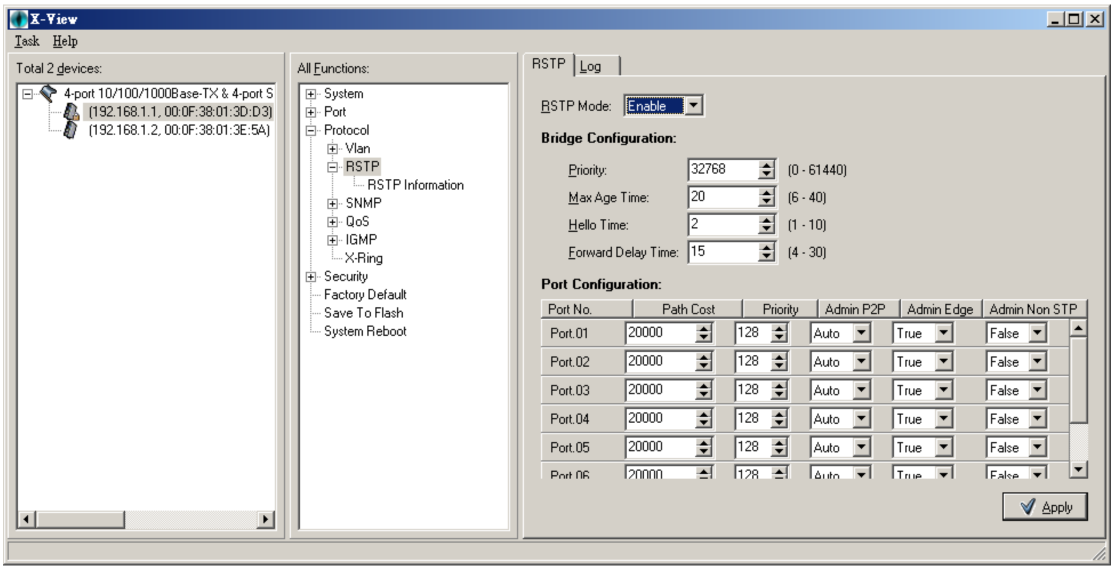
Bridge Configuration

- **RSTP mode:** user must enable or disable RSTP function before configure the related parameters
- **Priority (0-61440):** a value used to identify the root bridge. The bridge with the lowest value has the highest priority and is selected as the root. If the value changes, user must reboot the switch. The value must be multiple of 4096 according to the protocol standard rule.
- **Max Age (6-40):** the number of seconds a bridge waits without receiving Spanning Tree Protocol configuration messages before attempting a reconfiguration. Enter a value between 6 through 40.
- **Hello Time (1-10):** the time that controls switch sends out the BPDU packet to check RSTP current status. Enter a value between 1 through 10.
- **Forward Delay Time (4-30):** the number of seconds a port waits before changing from its Rapid Spanning-Tree Protocol learning and listening states to the forwarding state. Enter a value between 4 through 30.

RSTP - Port Configuration

You can configure path cost and priority of every port.

- Select the port in Port column.
- **Path Cost:** The cost of the path to the other bridge from this transmitting bridge at the specified port. Enter a number 1 through 200000000.
- **Priority:** Decide which port should be blocked by priority in LAN. Enter a number 0 through 240. The value of priority must be the multiple of 16.
- **P2P:** Some of the rapid state transactions that are possible within RSTP are dependent upon whether the port concerned can only be connected to exactly one other bridge (i.e. it is served by a point-to-point LAN segment), or can be connected to two or more bridges (i.e. it is served by a shared medium LAN segment). This function allows the P2P status of the link to be manipulated administratively. True is P2P enabling. False is P2P disabling.
- **Edge:** The port directly connected to end stations cannot create bridging loop in the network. To configure the port as an edge port, set the port to "True" status.
- **Non Stp:** The port includes the STP mathematic calculation. True is not including STP mathematic calculation. False is including the STP mathematic calculation.
- Click 'Apply'.



RSTP Mode: Enable

Bridge Configuration:

Priority:	32768	(0 - 61440)
Max Age Time:	20	(6 - 40)
Hello Time:	2	(1 - 10)
Forward Delay Time:	15	(4 - 30)

Port Configuration:

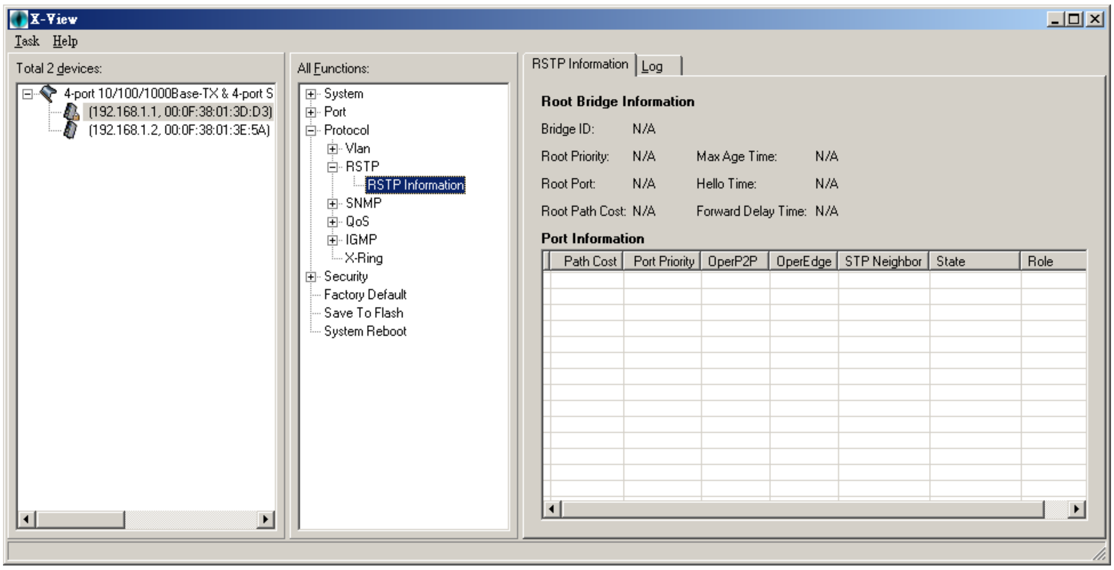
Port No.	Path Cost	Priority	Admin P2P	Admin Edge	Admin Non STP
Port.01	20000	128	Auto	True	False
Port.02	20000	128	Auto	True	False
Port.03	20000	128	Auto	True	False
Port.04	20000	128	Auto	True	False
Port.05	20000	128	Auto	True	False
Port.06	20000	128	Auto	True	False

Figure C.44: RSTP

Note *Follow the rule to configure the MAX Age, Hello Time, and Forward Delay Time.*
2 x (Forward Delay Time value –1) > = Max Age value >= 2 x (Hello Time value +1)

RSTP - Port Configuration

Here you can view the RSTP information.



Root Bridge Information

Bridge ID:	N/A		
Root Priority:	N/A	Max Age Time:	N/A
Root Port:	N/A	Hello Time:	N/A
Root Path Cost:	N/A	Forward Delay Time:	N/A

Port Information

Path Cost	Port Priority	OperP2P	OperEdge	STP Neighbor	State	Role

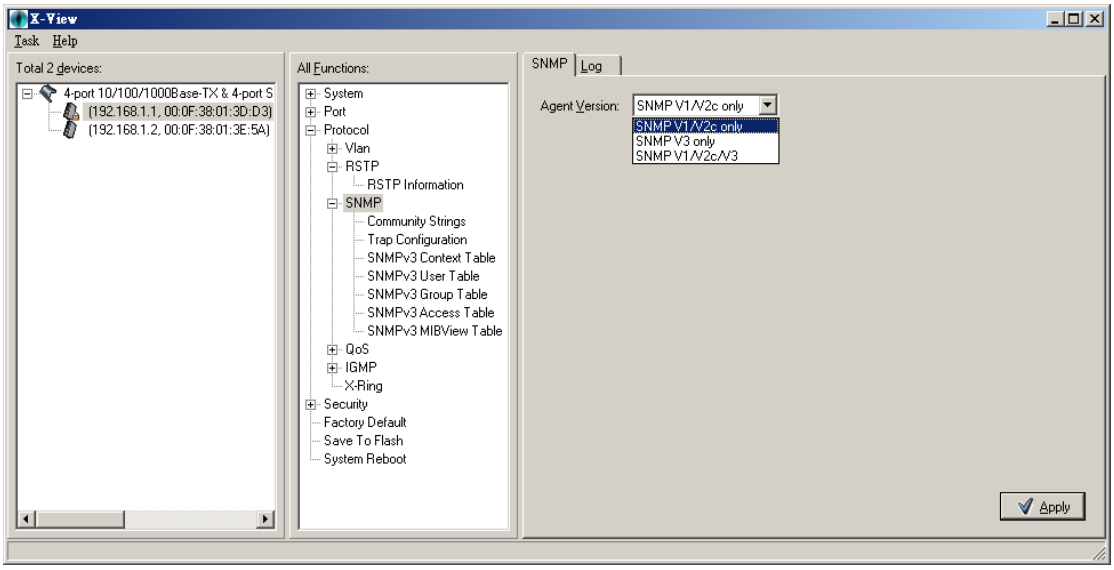
Figure C.45: RSTP Information

C.3.3 SNMP

Simple Network Management Protocol (SNMP) is the protocol developed to manage nodes (servers, workstations, routers, switches and hubs etc.) on an IP network. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth. Network management systems learn of problems by receiving traps or change notices from network devices implementing SNMP.

Agent Version

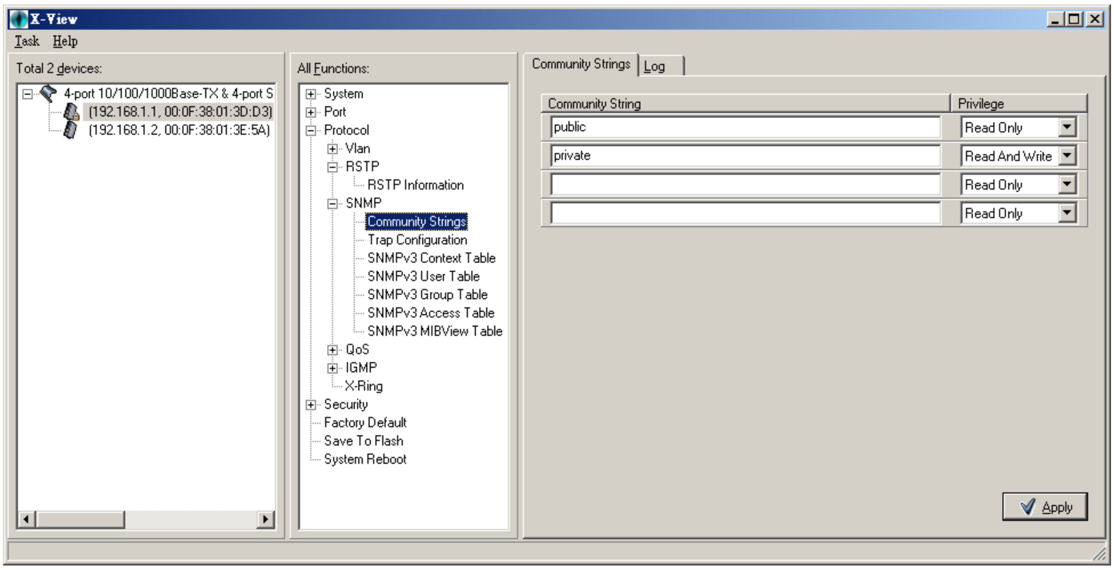
Select the SNMP version that you want to use it. And then click 'Apply' to switch to the selected SNMP version mode.



Agent Version: SNMP V1/V2c only

Figure C.46: SNMP

Community Strings



Community String	Privilege
public	Read Only
private	Read And Write
	Read Only
	Read Only

Figure C.47: Community Strings

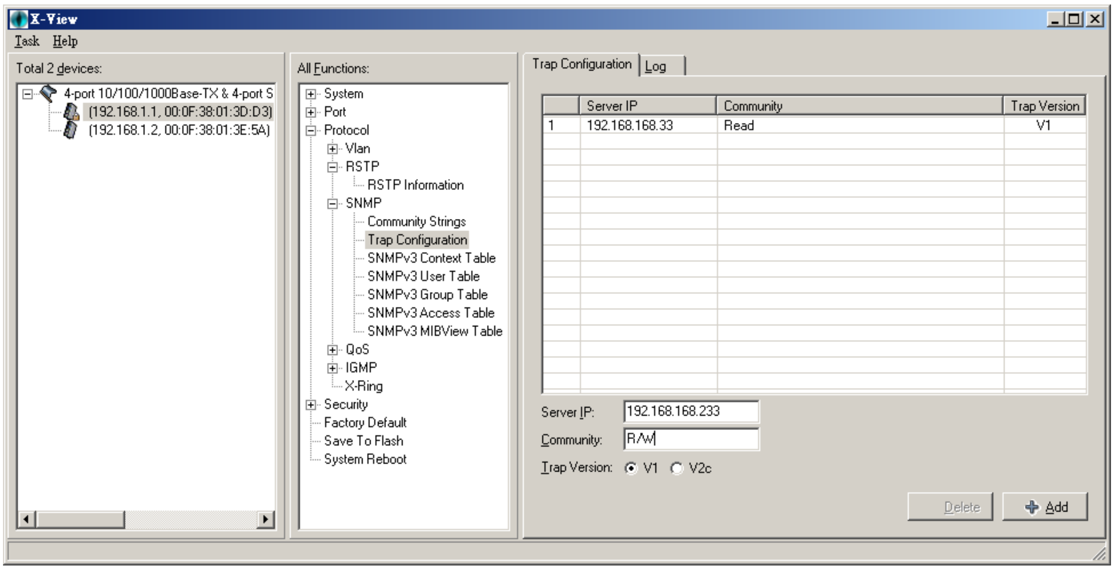
You can define new community string set and remove unwanted community string.

- **Community String:** Fill the name string.
- **Privilege:** 'Read only' enables requests that accompanied by this string to display MIB-object information. 'Read and Write' enables requests accompanied by this string to display MIB-object information and to set objects.
- Click 'Apply'.

Trap Configuration

A trap manager is a management station that receives traps, the system alerts generated by the switch. If no trap manager is defined, no traps will issue. Create a trap manager by entering the IP address of the station and a community string. To define management stations as trap manager and enter SNMP community strings and selects the SNMP version.

- **Server IP:** Enter the IP address of trap manager.
- **Community:** Enter the community string.
- **Trap Version:** Select the SNMP trap version type – v1 or v2c.
- Click 'Add'.
- To remove the community string, select the community string that you have defined and click 'Delete'. You cannot edit the name of the default community string set.



	Server IP	Community	Trap Version
1	192.168.168.33	Read	V1

Server IP: 192.168.168.233

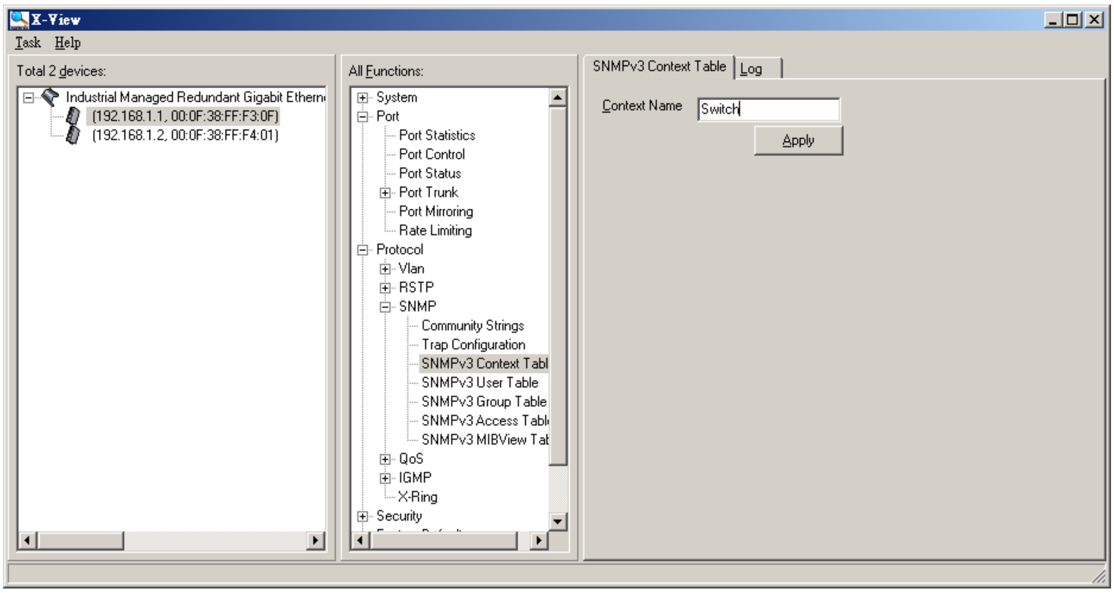
Community: R/W

Trap Version: ● V1 ○ V2c

Figure C.48: Trap Configuration

SNMPv3 Context Table

Configure SNMP v3 context table. Assign the context name of context table. Click 'Add' to add context name.



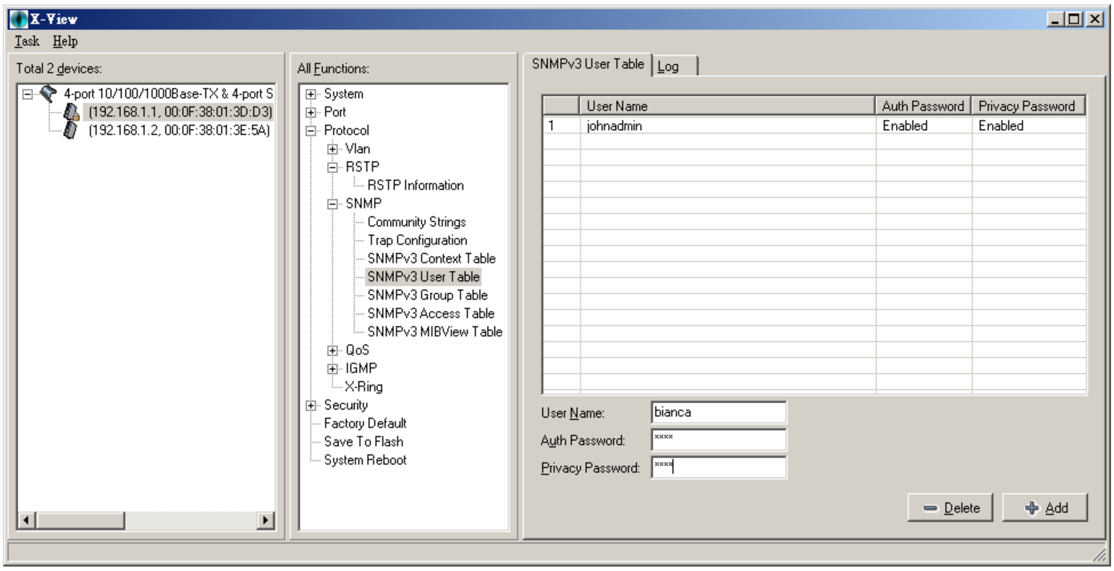
Context Name: Switch

Figure C.49: SNMPv3 Context Table

SNMPv3 User Table

Configure SNMP v3 user table..

- **User Name:** set up the user name.
- **Authentication Password:** set up the authentication password.
- **Privacy Password:** set up the private password.
- Click ‘Add’ to add context name.
- Click ‘Delete’ to remove unwanted context name.



	User Name	Auth Password	Privacy Password
1	johnadmin	Enabled	Enabled

User Name: bianca

Auth Password: ****

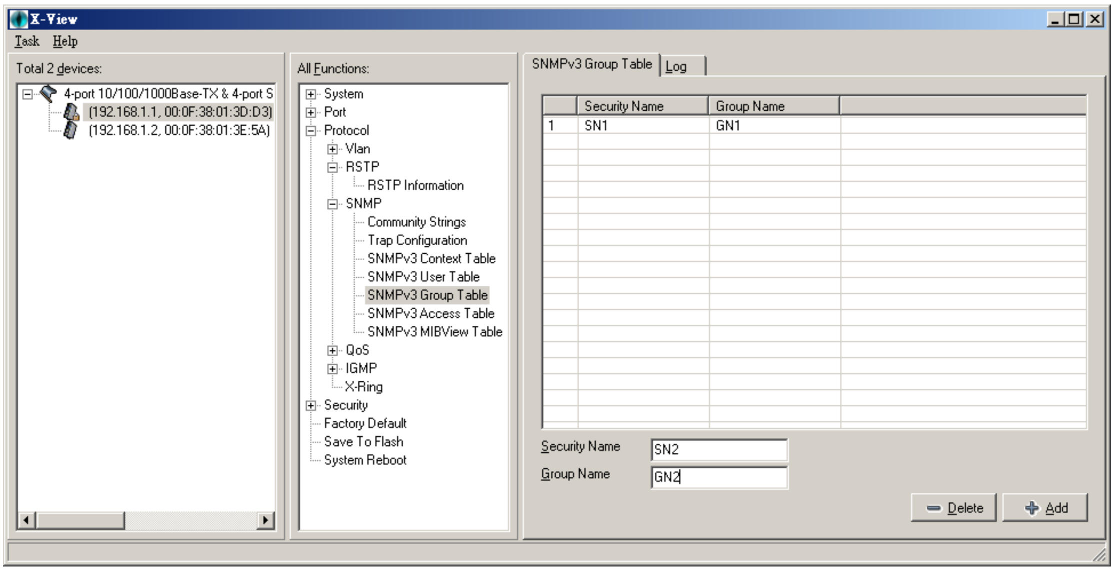
Privacy Password: ****

Figure C.50: SNMPv3 User Table

SNMPv3 Group Table

Configure SNMP v3 group table.

- **Security Name (User ID):** Assign the user name that you have set up in user table.
- **Group Name:** Set up the group name.
- Click ‘Add’ to add context name.
- Click ‘Delete’ to remove unwanted context name.



	Security Name	Group Name
1	SN1	GN1

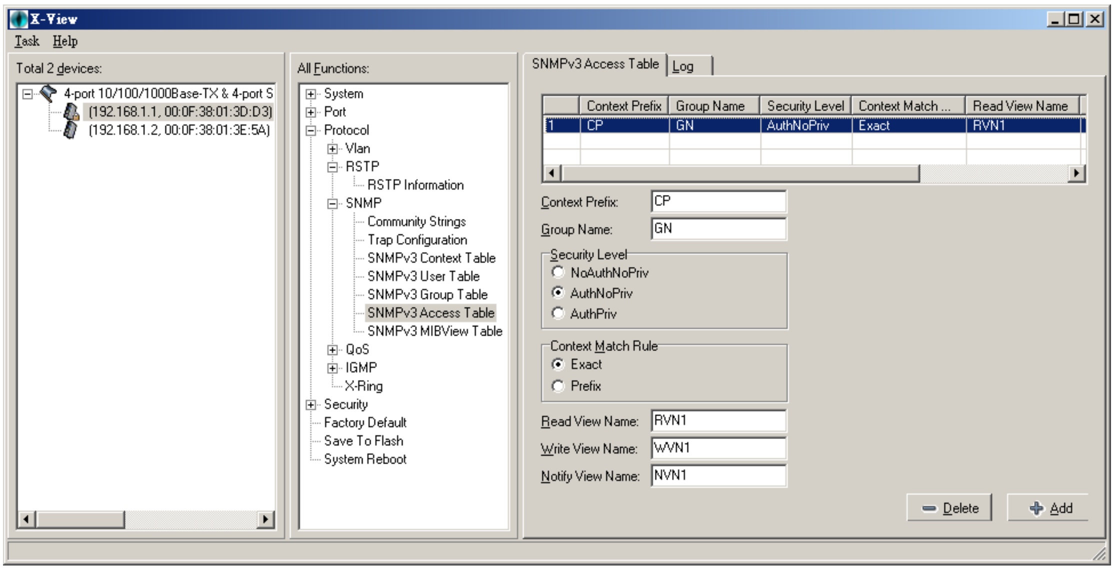
Security Name: SN2

Group Name: GN2

Figure C.51: SNMPv3 Group Table

SNMPv3 Access Table

Configure SNMP v3 access table.



	Context Prefix	Group Name	Security Level	Context Match ...	Read View Name
1	CP	GN	AuthNoPriv	Exact	RVN1

Context Prefix: CP

Group Name: GN

Security Level
- ○ NoAuthNoPriv
- ● AuthNoPriv
- ○ AuthPriv

Context Match Rule
- ● Exact
- ○ Prefix

Read View Name: RVN1

Write View Name: WVN1

Notify View Name: NVN1

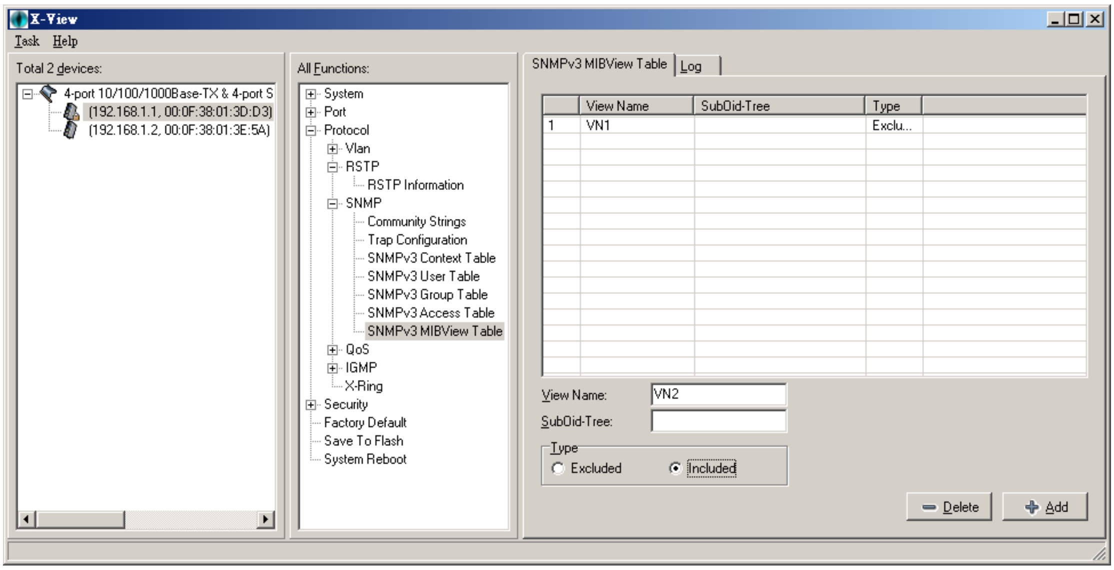
Figure C.52: SNMPv3 Access Table

- **Context Prefix:** Set up the context name.
- **Group Name:** Set up the group.
- **Security Level:** Set up the access level.
- **Context Match Rule:** Select the context match rule.
- **Read View Name:** Set up the read view.
- **Write View Name:** Set up the write view.
- **Notify View Name:** Set up the notify view.
- Click ‘Add’ to add context name.
- Click ‘Delete’ to remove unwanted context name.

SNMPv3 MIBview Table

Configure MIB view table.

- **ViewName:** Set up the name.
- **Sub-Oid Tree:** Fill the Sub OID.
- **Type:** Select the type – exclude or included.
- Click ‘Add’ to add context name.
- Click ‘Delete’ to remove unwanted context name.



	View Name	SubOid-Tree	Type
1	VN1		Exclu...

View Name: VN2

SubOid-Tree:

Type: ○ Excluded ● Included

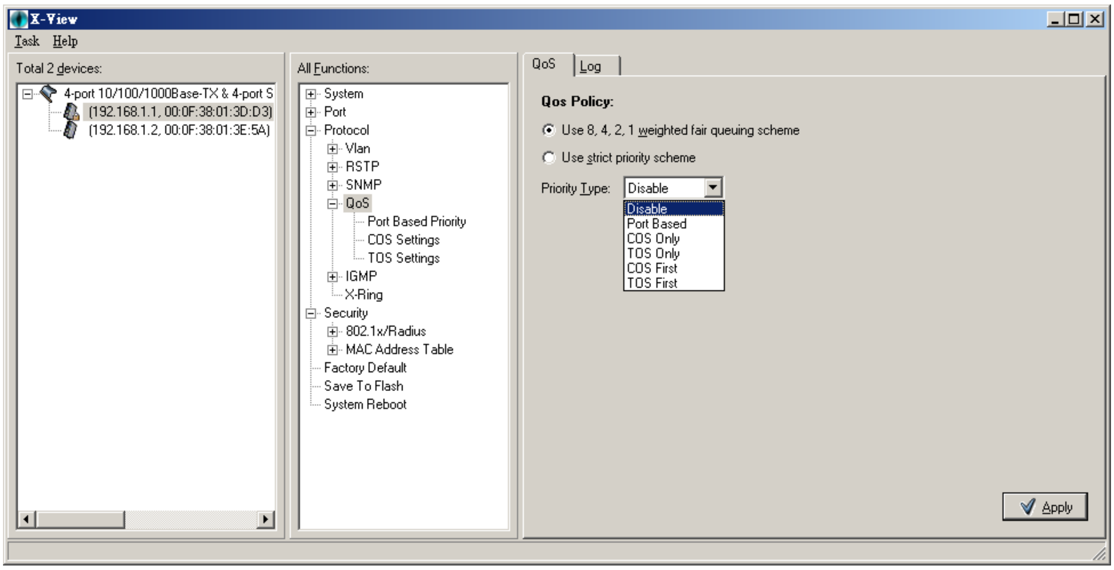
Figure C.53: SNMPv3 MIBView Table

C.3.4 QoS Configuration

You can configure Qos policy and priority setting, per port priority setting, COS and TOS setting.

QoS Policy and Priority Type

- **Qos Policy:** select the Qos policy rule.
    - Use an 8,4,2,1 weighted fair queuing scheme: The switch will follow 8:4:2:1 rate to process priority queue from High to Lowest queue. For example, as the system processes, 1 frame of the lowest queue, 2 frames of the low queue, 4 frames of the middle queue, and 8 frames of the high queue will be processed at the same time in accordance with the 8,4,2,1 policy rule.
    - Use a strict priority scheme: Always higher queue will be processed first, except higher queue is empty.
- **Priority Type:** there are 5 priority type selections available. Disable means no priority type is selected.
- **Port-base:** the port priority will follow the Port-base that you have assigned – High, middle, low, or lowest.
    - **COS only:** the port priority will only follow the COS priority that you have assigned.
    - **TOS only:** the port priority will only follow the TOS priority that you have assigned.
    - **COS first:** the port priority will follow the COS priority first, and then other priority rule.
    - **TOS first:** the port priority will follow the TOS priority first, and the other priority rule.
- Click 'Apply'.



Qos Policy:

● Use 8, 4, 2, 1 weighted fair queuing scheme

○ Use strict priority scheme

Priority Type: Disable

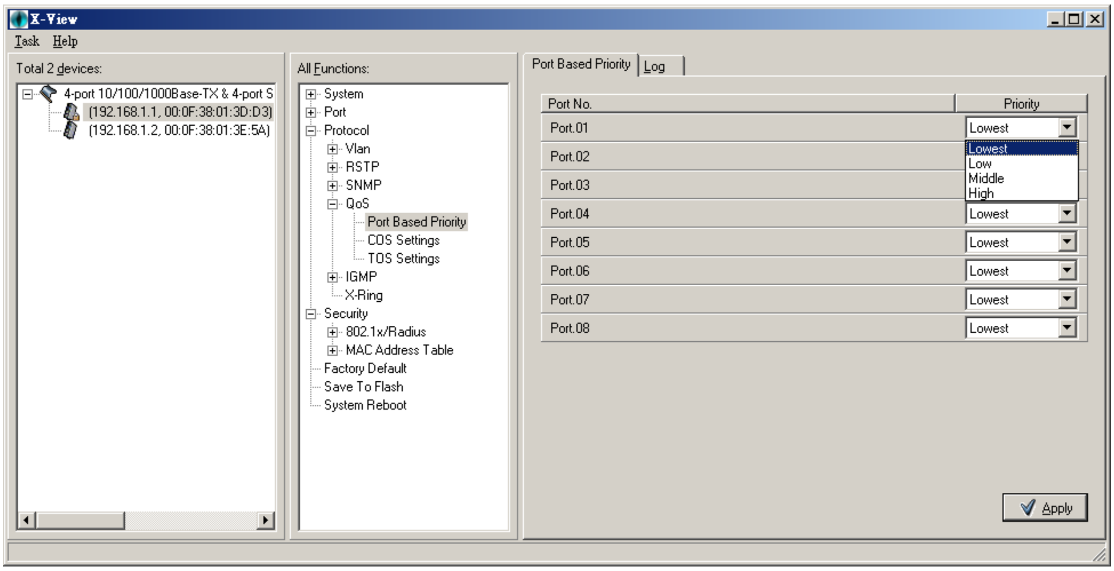
Disable
Port Based
COS Only
TOS Only
COS First
TOS First

Figure C.54: QoS

Port Base Priority

Configure per port priority level.

- **Port 1 ~ Port 10:** each port has 4 priority levels – High, Middle, Low, and Lowest.
- Click 'Apply'.



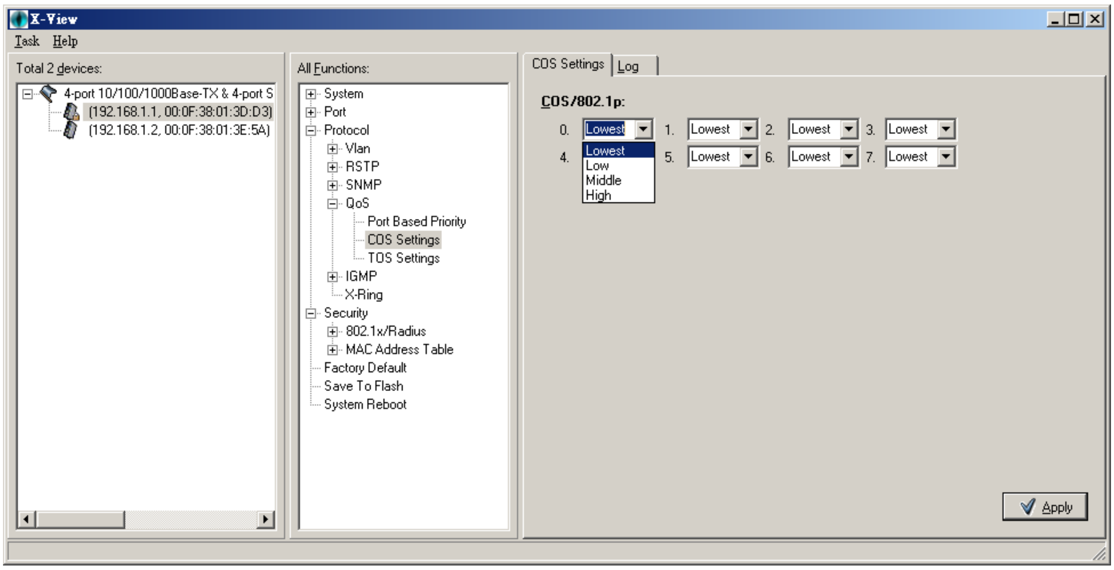
Port No.	Priority
Port.01	Lowest
Port.02	
Port.03	
Port.04	Lowest
Port.05	Lowest
Port.06	Lowest
Port.07	Lowest
Port.08	Lowest

Figure C.55: Port Based Priority

COS Settings

Set up the COS priority level.

- **COS priority:** Set up the COS priority level 0~7 –High, Middle, Low, Lowest.
- Click 'Apply'.



COS/802.1p:

0. Lowest 1. Lowest 2. Lowest 3. Lowest

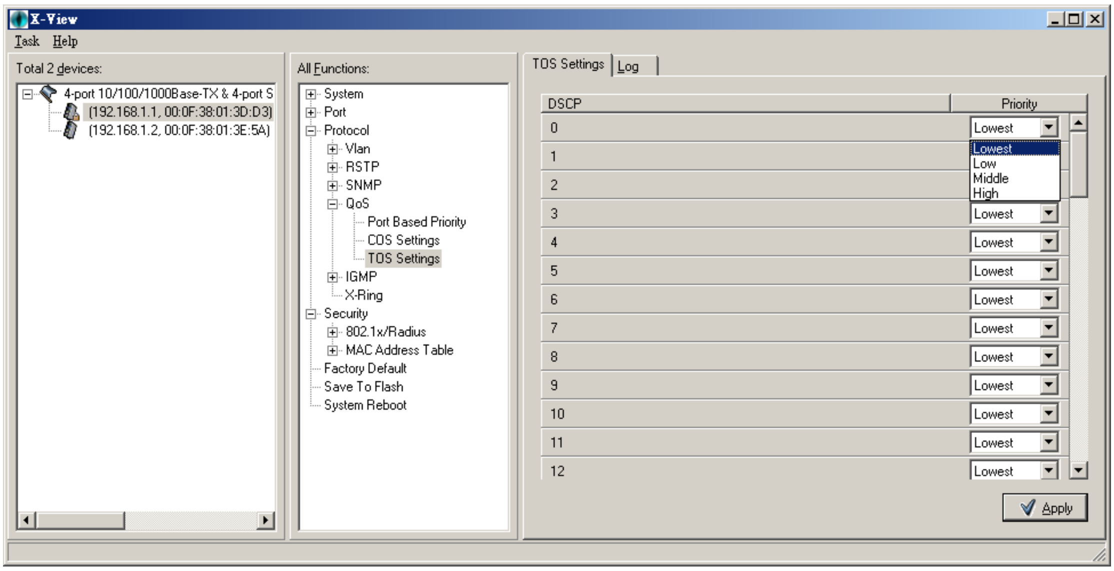
4. Lowest 5. Lowest 6. Lowest 7. Lowest

Figure C.56: COS Settings

TOS Settings

Set up the TOS priority.

- **TOS priority:** the system provides 0~63 TOS priority level. Each level has 4 types of priority – high, middle, low, and lowest. The default value is “Lowest” priority for each level. When the IP packet is received, the system will check the TOS level value in the IP packet that has received. For example, user set the TOS level 25 is high. The port 1 is following the TOS priority policy only. When the port 1 packet received, the system will check the TOS value of the received IP packet. If the TOS value of received IP packet is 25(priority = high), and then the packet priority will have highest priority.
- Click ‘Apply’.



DSCP	Priority
0	Lowest
1	
2	
3	Lowest
4	Lowest
5	Lowest
6	Lowest
7	Lowest
8	Lowest
9	Lowest
10	Lowest
11	Lowest
12	Lowest

Figure C.57: TOS Settings

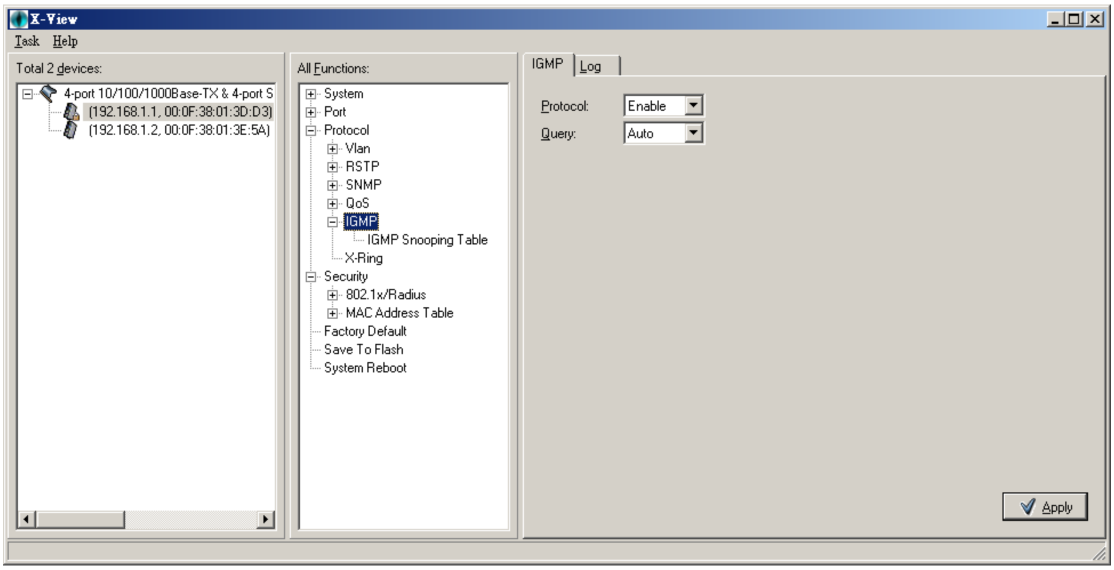
IGMP Configuration

The Internet Group Management Protocol (IGMP) is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of the IP multicast specification, like ICMP for unicast connections. IGMP can be used for online video and gaming, and allows more efficient use of resources when supporting these uses.
IGMP have three fundamental types of message as follows:

Table 3.19: IGMP types

Message	Description
Query	A message sent from the querier (IGMP router or switch) asking for a response from each host belonging to the multicast group.
Report	A message sent by a host to the querier to indicate that the host wants to be or is a member of a given group indicated in the report message.
Leave Group	A message sent by a host to the querier to indicate that the host has quit being a member of a specific multicast group.

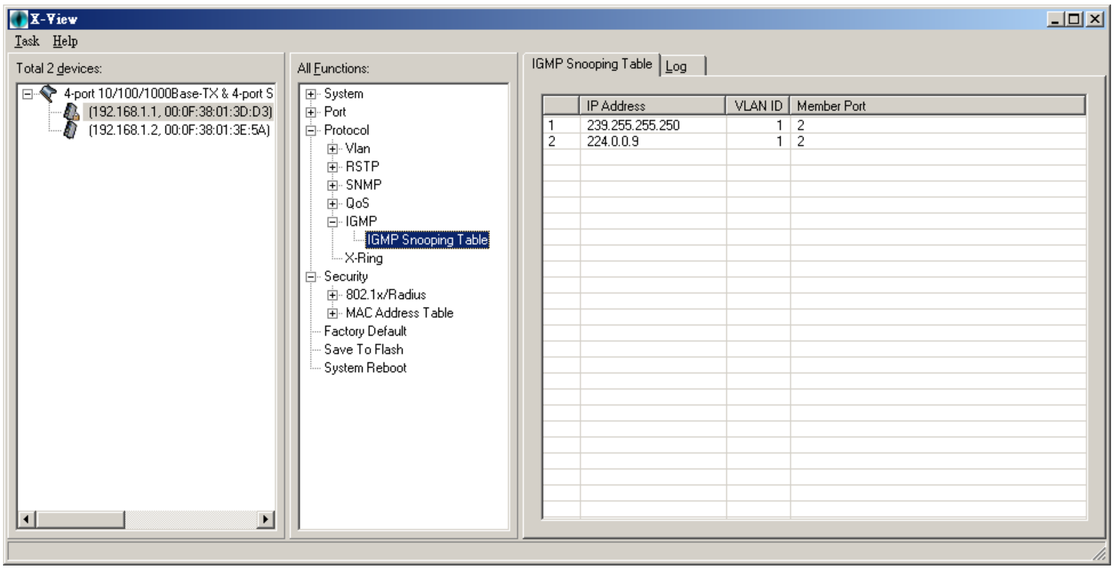
The switch support IP multicast, you can enable IGMP protocol on web management's switch setting advanced page, then displays the IGMP snooping information. IP multicast addresses range are from 224.0.0.0 through 239.255.255.255.



Protocol: Enable
Query: Auto

Figure C.58: IGMP

- **IGMP Protocol:** Enable or disable the IGMP protocol.
- **IGMP Query:** Select the IGMP query function as Enable or Auto to set the switch as a querier for IGMP version 2 multicast network.
- Click 'Apply'.



	IP Address	VLAN ID	Member Port
1	239.255.255.250	1	2
2	224.0.0.9	1	2

Figure C.59: IGMP Snooping Table

X-Ring

X-Ring provides a faster redundant recovery than Spanning Tree topology. The action is similar to STP or RSTP, but the algorithms not the same.

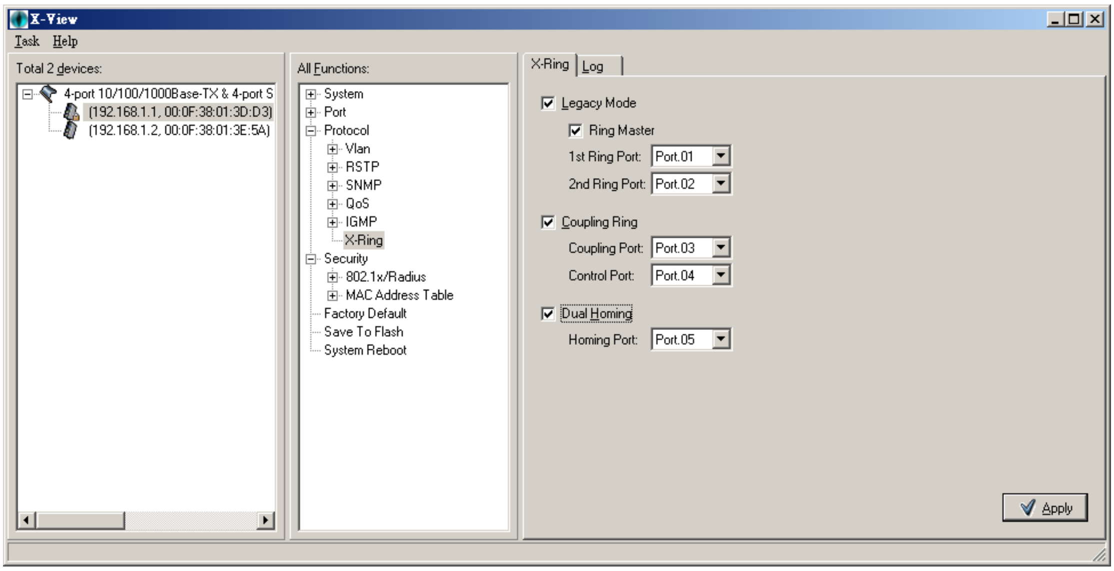
In the X-Ring topology, every switch should enable X-Ring function and assign two member ports in the ring. Only one switch in the X-Ring group would be set as a master switch, one of its path would be blocked, called backup port, and another port is called working port. Other switches in the X-Ring group are called working switches and their two member ports are called working ports. When the failure of network connection occurs, the backup port will automatically become a working port to recovery the failure.

The switch supports the function and interface for setting the switch as the ring master or slave mode. The ring master can negotiate and place command to other switches in the X-Ring group. If there are 2 or more switches in master mode, then software will select the switch with lowest MAC address number as the ring master. The X-Ring master ring mode will be enabled by the X-Ring configuration interface. Also, user can identify the switch as the ring master from the R.M. LED panel of the LED panel on the switch.

The system also supports the coupling ring that can connect 2 or more X-Ring group for the redundant backup function and dual homing function that prevent connection lose between X-Ring group and upper level/core switch.

- **Legacy Mode**: To enable the X-Ring function. Marking the check box to enable the X-Ring function.
- **Enable Ring Master**: Mark the check box for enabling this machine to be a ring master.
- **1st & 2nd Ring Ports**: Pull down the selection menu to assign two ports as the member ports. 1st Ring Port is the working port and 2nd Ring Port is the backup port. When 1st Ring Port fails, the system will automatically upgrade the 2nd Ring Port to be the working port.
- **Enable Coupling Ring**: To enable the coupling ring function. Marking the check box to enable the coupling ring function.
- **Coupling port**: Assign the member port.
- **Control port**: Set the switch as the master switch in the coupling ring.
- **Enable Dual Homing**: Set up one of port on the switch to be the Dual Homing port. In an X-Ring group, maximum Dual Homing port is one. Dual Homing only work when the X-Ring function enable.

- And then, click ‘Apply’ to apply the configuration.



X-View

Total 2 devices:

4-port 10/100/1000Base-TX & 4-port S
(192.168.1.1, 00:0F:38:01:3D:D3)
(192.168.1.2, 00:0F:38:01:3E:5A)

All Functions:

System
Port
Protocol
Vlan
RSTP
SNMP
QoS
IGMP
X-Ring
Security
802.1x/Radius
MAC Address Table
Factory Default
Save To Flash
System Reboot

X-Ring | Log

☑ Legacy Mode

☑ Ring Master

1st Ring Port: Port.01

2nd Ring Port: Port.02

☑ Coupling Ring

Coupling Port: Port.03

Control Port: Port.04

☑ Dual Homing

Homing Port: Port.05

Figure C.60: X-Ring

C.4 Security

In this section, you can configure 802.1x and MAC address table.

C.4.1 802.1x/RADIUS

802.1x is an IEEE authentication specification that allows a client to connect to a wireless access point or wired switch but prevents the client from gaining access to the Internet until it provides authority, like a user name and password that are verified by a separate server.

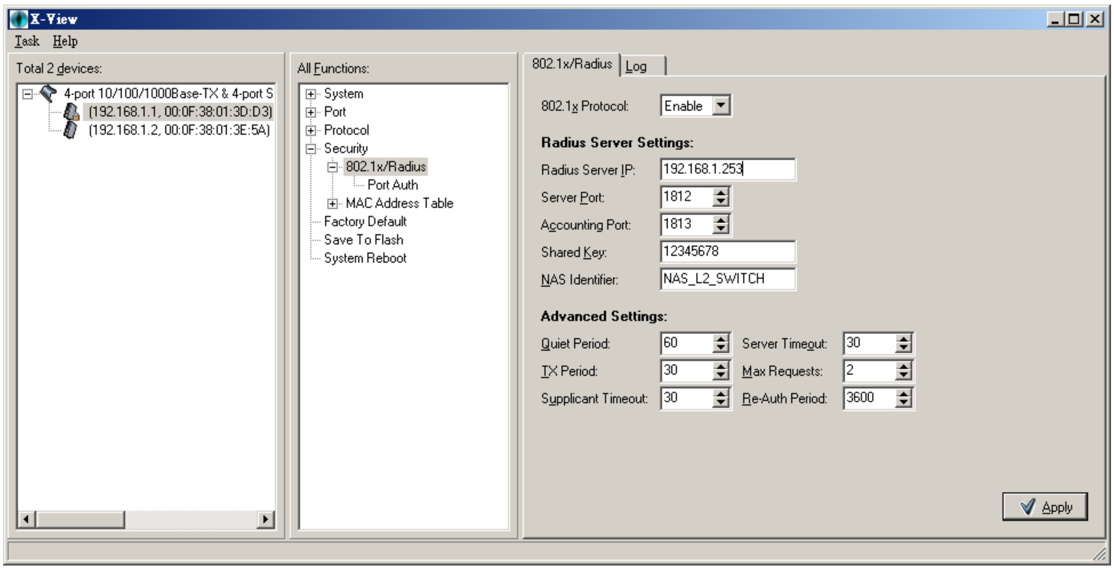
After enabling the IEEE 802.1X function, you can configure the parameters of this function.

Radius Server Settings:

- **IEEE 802.1x Protocol:** .enable or disable 802.1x protocol.
- **Radius Server IP:** set the Radius Server IP address.
- **Server Port:** set the UDP destination port for authentication requests to the specified Radius Server.
- **Accounting Port:** set the UDP destination port for accounting requests to the specified Radius Server.
- **Shared Key:** set an encryption key for using during authentication sessions with the specified radius server. This key must match the encryption key used on the Radius Server.
- **NAS, Identifier:** set the identifier for the radius client.

Advanced Settings:

- **Quiet Period:** set the period during which the port doesn't try to acquire a supplicant.
- **TX Period:** set the period the port wait for retransmit next EAPOL PDU during an authentication session.
- **Supplicant Timeout:** set the period of time the switch waits for a supplicant response to an EAP request.
- **Server Timeout:** set the period of time the switch waits for a server response to an authentication request.
- **Max Requests:** set the number of authentication that must time-out before authentication fails and the authentication session ends.
- **Reauth period:** set the period of time after which clients connected must be re-authenticated.
- Click 'Apply'.



802.1x Protocol: Enable

Radius Server Settings:

Radius Server IP: 192.168.1.253

Server Port: 1812

Accounting Port: 1813

Shared Key: 12345678

NAS Identifier: NAS_L2_SWITCH

Advanced Settings:

Quiet Period: 60 Server Timeout: 30

TX Period: 30 Max Requests: 2

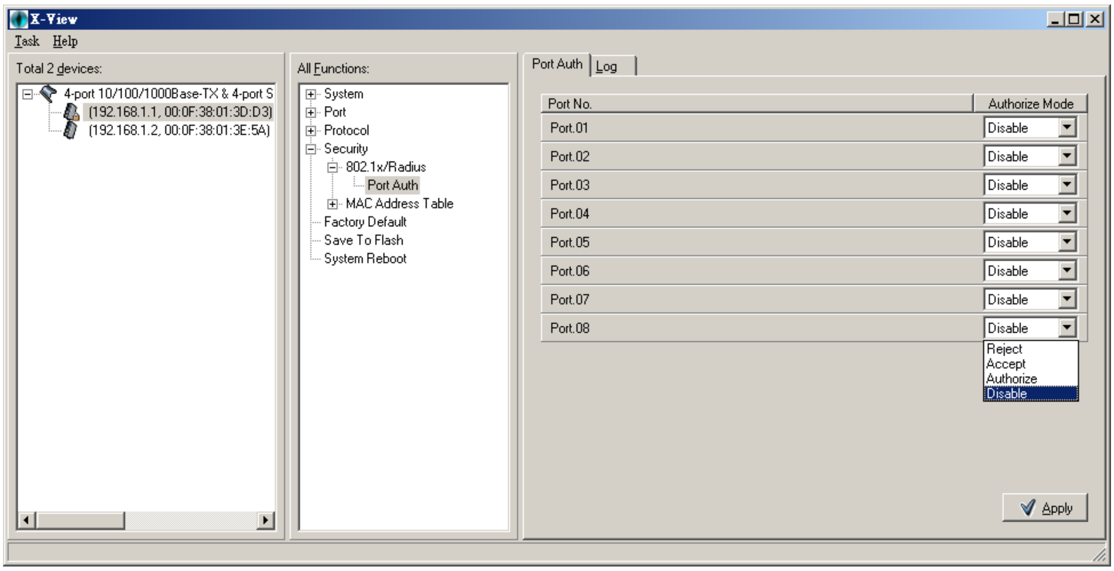
Supplicant Timeout: 30 Re-Auth Period: 3600

Figure C.61: 802.1x/RADIUS

Port Auth

You can configure 802.1x authentication state for each port. The State provides Disable, Accept, Reject and Authorize.

- **Reject:** the specified port is required to be held in the unauthorized state.
- **Accept:** the specified port is required to be held in the Authorized state.
- **Authorized:** the specified port is set to the Authorized or Unauthorized state in accordance with the outcome of an authentication exchange between the Supplicant and the authentication server.
- **Disable:** The specified port is required to be held in the Authorized state.
- Click ‘Apply’.



Port No.	Authorize Mode
Port.01	Disable
Port.02	Disable
Port.03	Disable
Port.04	Disable
Port.05	Disable
Port.06	Disable
Port.07	Disable
Port.08	Disable

Figure C.62: Port Auth

C.4.2 MAC Address Table

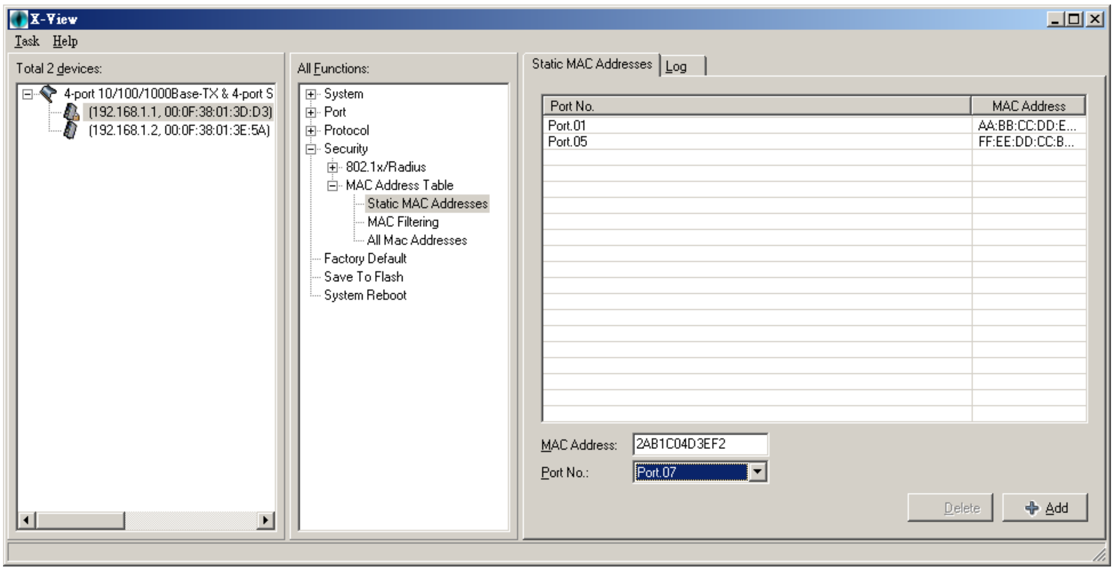
Use the MAC address table to ensure the port security.

You can add a static MAC address; it remains in the switch's address table, regardless of whether the device is physically connected to the switch. This saves the switch from having to re-learn a device's MAC address when the disconnected or powered-off device is active on the network again. You can add / modify / delete a static MAC address.

Static MAC Address

You can add static MAC address in the switch MAC table here.

- **MAC Address:** Enter the MAC address of the port that should permanently forward traffic, regardless of the device network activity.
- **Port No.:** pull down the selection menu to select the port number.
- Click 'Add'.
- If you want to delete the MAC address from filtering table, select the MAC address and click 'Delete'.



Port No.	MAC Address
Port.01	AA:BB:CC:DD:E...
Port.05	FF:EE:DD:CC:B...

MAC Address: 2AB1C04D3EF2

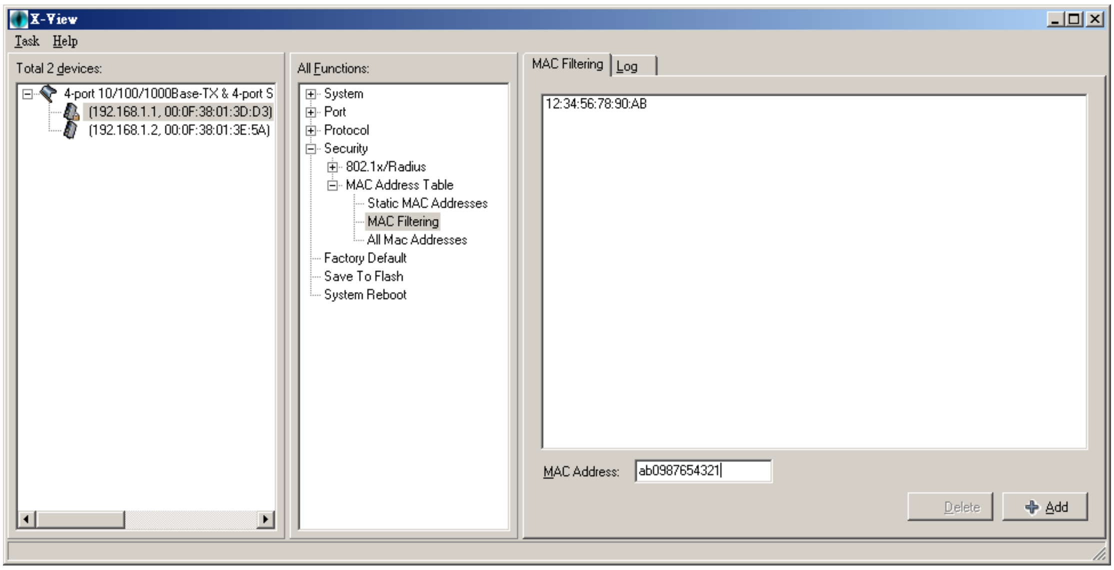
Port No.: Port.07

Figure C.63: Static MAC Address

MAC Filtering

By filtering MAC address, the switch can easily filter pre-configured MAC address and reduce the un-safety. You can add and delete filtering MAC address via this function.

- MAC Address: Enter the MAC address that you want to filter.
- Click 'Add'.
- If you want to delete the MAC address from filtering table, select the MAC address and click 'Delete'.



12:34:56:78:90:AB

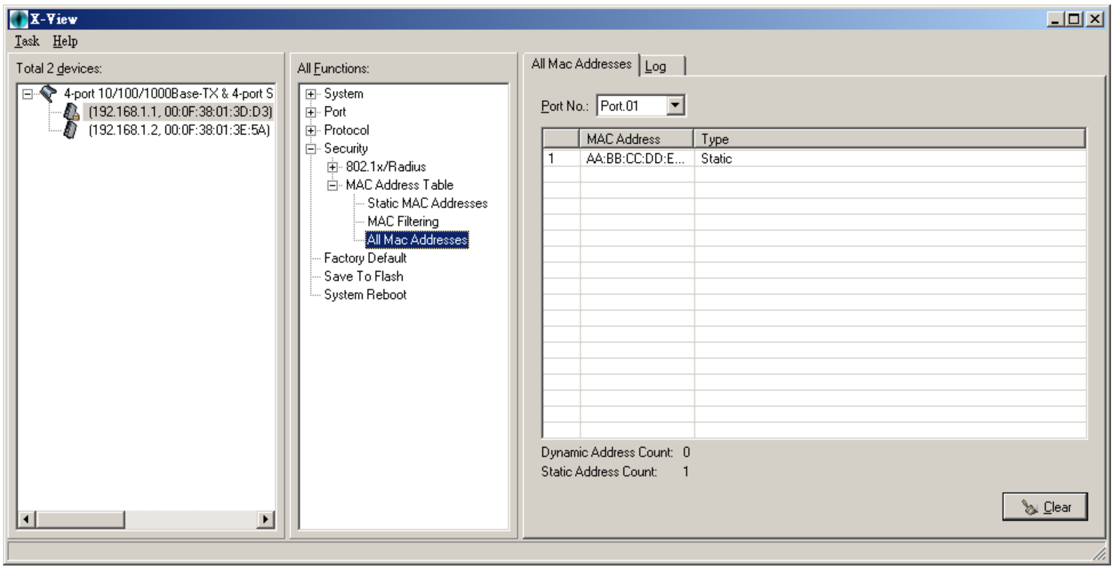
MAC Address: ab0987654321

Figure C.64: MAC Filtering

All MAC Addresses

You can view the port of connected device's MAC address and related devices' MAC address.

- Select the port.
- The selected port of the static MAC address information will be displayed here.
- Click 'Clear' button to clear the current port static MAC address information in the MAC table.



Port No.: Port.01

	MAC Address	Type
1	AA:BB:CC:DD:E...	Static

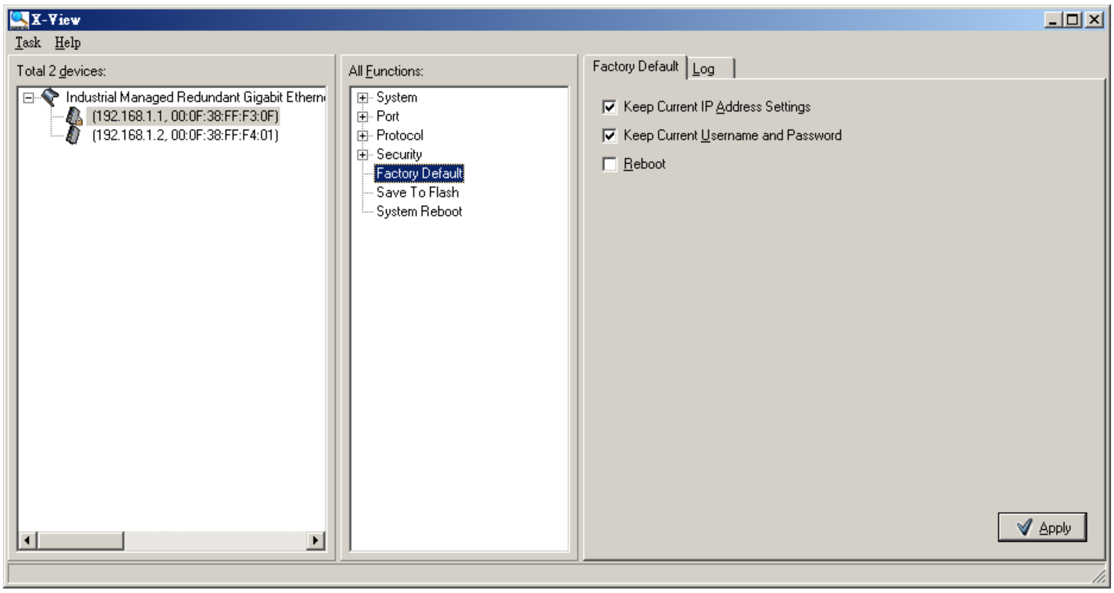
Dynamic Address Count: 0

Static Address Count: 1

Figure C.65: All MAC Address

C.5 Factory Default

Reset switch to default configuration. Mark the check boxes to keep current IP, User Name and Password while rebooting. Click ‘Apply button to reset all configurations to the default value.



☑ Keep Current IP Address Settings
☑ Keep Current Username and Password
□ Reboot

Figure C.66: Factory Default

C.6 Save To Flash

Save all configurations that you have made in the system. To ensure the all configuration will be saved. Click ‘Save’ button to save the entire configuration to the flash memory.

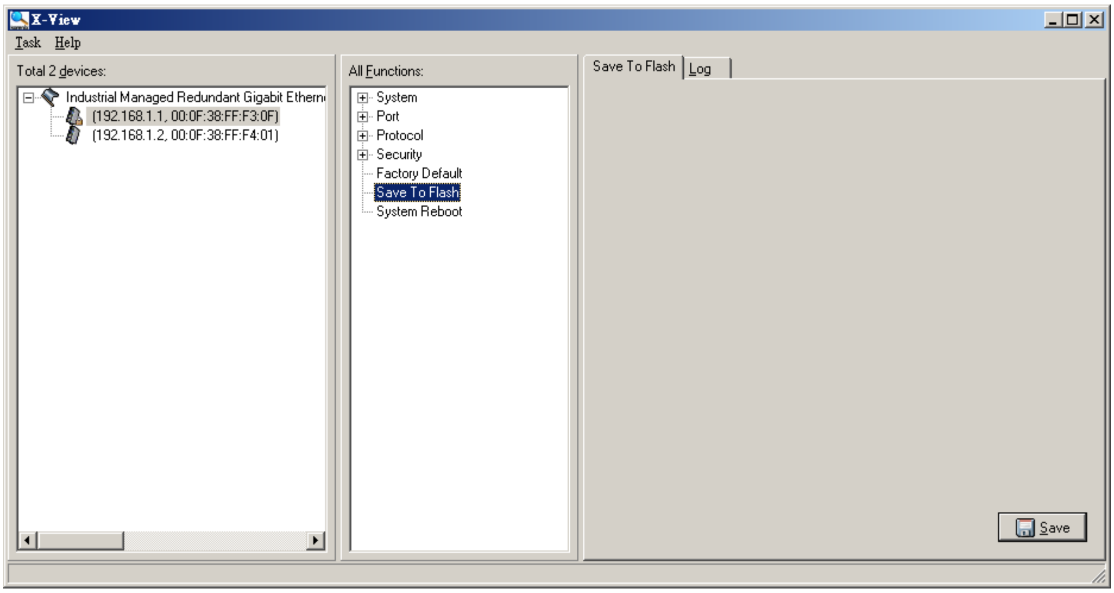


Figure C.67: Save to Flash

C.7 System Reboot

Reboot the switch in software reset. Click ‘Reboot’ button to reboot the system.

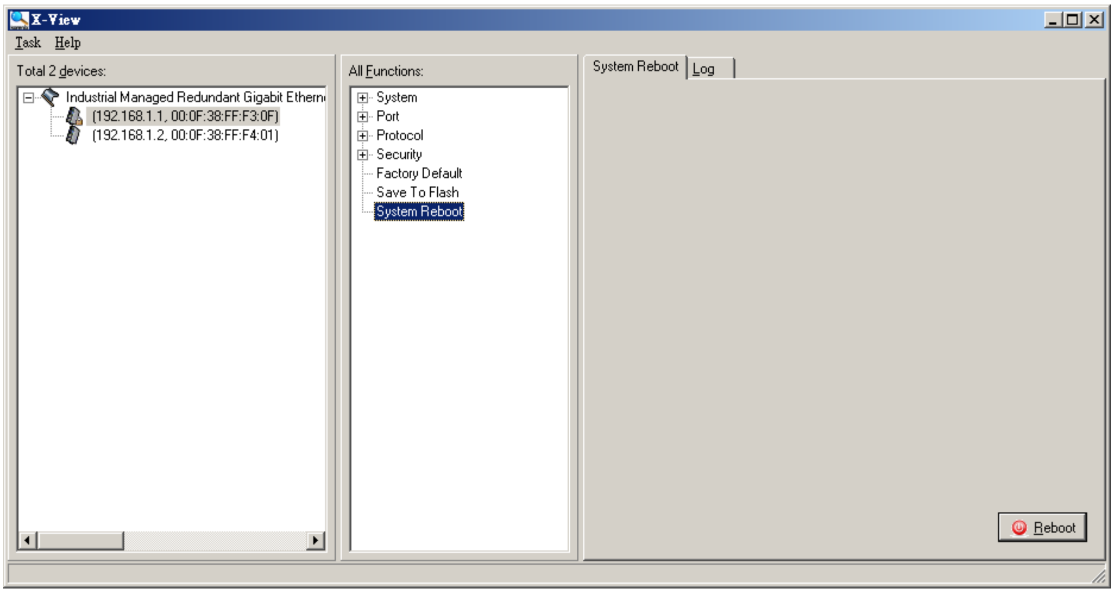


Figure C.68: System Reboot